



日本国特許庁  
JAPAN PATENT OFFICE

#8  
2-5-03  
JM

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出願年月日

Date of Application:

2001年 6月 5日

出願番号

Application Number:

特願2001-169326

[ST.10/C]:

[JP2001-169326]

出願人

Applicant(s):

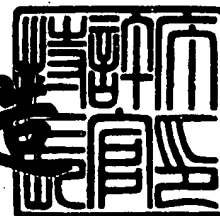
シーア・インサイト・セキュリティ株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2002年 3月22日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2002-3019905

【書類名】 特許願

【整理番号】 ID010220

【提出日】 平成13年 6月 5日

【あて先】 特許庁長官殿

【発明の名称】 セキュリティ管理サーバおよびこれと連携して動作する  
ホストサーバ

【請求項の数】 57

【発明者】

    【住所又は居所】 東京都目黒区下目黒 6 - 2 0 - 6 - 2 0 3

    【氏名】 向井 徹

【発明者】

    【住所又は居所】 東京都町田市玉川学園 5 - 1 8 - 2 1

    【氏名】 石田 明

【発明者】

    【住所又は居所】 東京都練馬区石神井台 3 - 2 4 - 2 6 - 3 0 1

    【氏名】 足立 正浩

【発明者】

    【住所又は居所】 東京都杉並区荻窪 5 - 2 9 - 1 7 - 1 1 0 4

    【氏名】 小池 英樹

【発明者】

    【住所又は居所】 東京都調布市飛田給 2 - 4 6 - 1 2 - 2 0 5

    【氏名】 高田 哲司

【発明者】

    【住所又は居所】 東京都足立区西綾瀬 3 - 3 9 - 7 - 6 0 2

    【氏名】 溜田 英二

【特許出願人】

    【識別番号】 501051516

    【氏名又は名称】 シーア・インサイト・セキュリティ株式会社

【代理人】

【識別番号】 100071283

【弁理士】

【氏名又は名称】 一色 健輔

【選任した代理人】

【識別番号】 100084906

【弁理士】

【氏名又は名称】 原島 典孝

【選任した代理人】

【識別番号】 100094042

【弁理士】

【氏名又は名称】 鈴木 知

【選任した代理人】

【識別番号】 100098523

【弁理士】

【氏名又は名称】 黒川 恵

【先の出願に基づく優先権主張】

【出願番号】 特願2001- 58736

【出願日】 平成13年 3月 2日

【手数料の表示】

【予納台帳番号】 011785

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【物件名】 委任状 1

【援用の表示】 平成13年6月5日提出の包括委任状

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ管理サーバおよびこれと連携して動作するホストサーバ

【特許請求の範囲】

【請求項 1】 所定の LAN 内に設置され、

前記 LAN 内で稼働する監視対象装置が前記 LAN を通じて行う通信に関連する情報を収集する手段と、

収集した前記通信関連情報から前記 LAN におけるセキュリティ管理に有用な情報を抽出しその情報を所定の形態に視覚化した映像を生成する手段と、

前記映像を監視装置に送信する手段と、

を備えることを特徴とするセキュリティ管理サーバ。

【請求項 2】 請求項 1 に記載のセキュリティ管理サーバであって、前記通信関連情報に基づいて前記監視対象装置のセキュリティ上の異常を検知する手段と、その異常を検知した場合にその旨やその内容を前記映像に反映させる手段と、を備えることを特徴とする。

【請求項 3】 請求項 1 または 2 に記載のセキュリティ管理サーバであって、前記通信関連情報が前記監視対象装置に記憶管理されているログ情報であり、前記ログ情報を前記 LAN を通じて収集する手段を備えることを特徴とする。

【請求項 4】 請求項 1 ～ 3 のいずれかに記載のセキュリティ管理サーバであって、

前記 LAN がインターネットなどの外部のネットワークにも接続し、

前記映像を生成する手段が、

前記監視対象装置と、これと通信する前記外部のネットワークで稼働する装置と、これらの装置を利用中のユーザと、前記 LAN 内外の各装置間で行われる通信とを、それぞれ所定のオブジェクトに視覚化した映像を生成する手段を備えることを特徴とする。

【請求項 5】 請求項 4 に記載のセキュリティ管理サーバであって、

前記映像を生成する手段が、

前記各オブジェクトを所定の基準に従ってグループ分けし、各グループ別に階

層的に視覚化した映像を生成する手段を備えることを特徴とする。

【請求項 6】 請求項 5 に記載のセキュリティ管理サーバであって、前記基準が、前記各装置と前記 LAN との間の信頼度に基づくものであることを特徴とする。

【請求項 7】 請求項 3 ～ 6 のいずれかに記載のセキュリティ管理サーバであって、

前記映像を生成する手段が、

前記各監視対象装置において行われた各種の処理がその内容と実行日時とを含むテキストメッセージの形式で行別記載されて構成されるログ情報に基づいて、テキストメッセージをそのまま表示するエリアと、所定の文字列の前記ログ情報中における出現頻度をグラフ表示したエリアと、前記文字列の所定単位期間ごとの出現頻度を時系列的にグラフ表示したエリアと、前記テキストメッセージの各行の長さをグラフ表示したエリアと、を備えて構成される映像を生成する機能を備えることを特徴とする。

【請求項 8】 請求項 3 ～ 7 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置が、

前記ログ情報の実体であるログファイルを、正本ファイルと、これとリアルタイムに同一内容に維持管理された複数の副本ファイルとの複数立てで管理し、前記各ファイルを当該監視対象装置内の記憶手段に適宜に区画された複数の記憶場所に分散して記憶管理する手段と、前記各副本ファイルを他の前記記憶場所に適宜移送する手段と、前記正副両ログファイルにセキュリティ上の異常がないかどうかを検知する手段と、異常を検知した場合にその旨やその内容を前記セキュリティ管理サーバに通知する手段とを有し、

前記映像を生成する手段が、前記監視対象装置から通知される、前記異常を検知した旨やその内容を、前記映像に反映させる手段を備えることを特徴とする。

【請求項 9】 請求項 4 ～ 8 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータから送られてくる更新データを受信する手段と、前記映像を生成する手段を提供するソフトウエ

アの内容を前記更新データにより更新する手段とを備えることを特徴とする。

【請求項10】 請求項4～9のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報をこのコンピュータとの間で送受信する手段を備えることを特徴とする。

【請求項11】 請求項4～10のいずれかに記載のセキュリティ管理サーバであって、前記ログ情報の収集対象となる前記監視対象装置についての情報や、前記映像を生成する手段で利用・参照される情報などの各種の設定登録情報を記憶管理する手段を備え、

前記外部のネットワークで稼働する所定のコンピュータと通信し、前記設定登録情報を前記コンピュータとの間で送受信する手段を備えることを特徴とする。

【請求項12】 請求項4～11のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報や当該セキュリティ管理サーバ自身が記憶管理している自身のログ情報に基づいて、前記監視対象装置や当該セキュリティ管理サーバ自身のセキュリティ上の異常を検知する手段と、

異常を検知した場合にその旨やその内容を、前記コンピュータとの間で送受信する手段を備えることを特徴とする。

【請求項13】 請求項1～12のいずれかに記載のセキュリティ管理サーバであって、

前記各監視対象装置との間でTCP/IPプロトコルに基づいて通信する手段と、

前記LAN内の前記各監視対象装置からの要求に応じて所定のIPアドレスを割り当てるとともにそのIPアドレスと前記各監視対象装置のMACアドレスとの対応づけの履歴を記載した割当履歴を記憶管理する手段と、

収集した前記通信関連情報をそれがどの前記監視対象装置に関する通信関連情報であるかを特定するIPアドレスを付帯させて記憶管理する手段と、

前記割当履歴において同一のMACアドレスに対応づけられたIPアドレスが付帯する前記通信関連情報を、同一の前記監視対象装置に関する通信関連情報で

あるとして取り扱う手段と、を備えることを特徴とする。

【請求項14】 請求項13に記載のセキュリティ管理サーバであって、前記LAN内で稼働する他のセキュリティ管理サーバとの間で前記割当履歴を相互に送受信する手段と、

受信した他のセキュリティ管理サーバにおける前記割当履歴と、自身が記憶管理している前記割当履歴とを統合管理し、これら割当履歴において同一のMACアドレスに対応づけられたIPアドレスが付帯する前記通信関連情報を、同一の前記監視対象装置に関する通信関連情報であるとして取り扱う手段と、を備えることを特徴とする。

【請求項15】 請求項13または14に記載のセキュリティ管理サーバであって、前記割当履歴に対応づけて記述されるMACアドレスとIPアドレスの各組み合わせにはそのIPアドレスの有効期間情報が付帯し、この有効期間情報と収集した前記通信関連情報に付帯して記録されている当該通信関連情報の生成日時とを比較して、前記生成日時において前記通信関連情報に付帯するIPアドレスが対応づけられていたMACアドレスを特定する手段を備えることを特徴とする。

【請求項16】 請求項9における前記所定のコンピュータとして機能するホストサーバであって、前記更新データを適宜前記セキュリティ管理サーバに送信する手段を備えることを特徴とする。

【請求項17】 請求項10における前記所定のコンピュータとして機能するホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記通信関連情報を記憶管理する手段を備えることを特徴とする。

【請求項18】 請求項17に記載の前記ホストサーバであって、記憶管理している前記通信関連情報を前記セキュリティ管理サーバに送信する手段を備えることを特徴とする。

【請求項19】 請求項17または18に記載の前記ホストサーバであって、記憶管理している前記通信関連情報に基づいて前記監視対象装置についてのセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を該当のLAN内に設置されたセキュリティ管理サーバに送信する手段を備える

ことを特徴とする。

【請求項 20】 請求項 17～19 のいずれかに記載のホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記各種設定情報、もしくは、前記異常を検知した旨やその内容を受信してこれを記憶管理する手段を備えることを特徴とする。

【請求項 21】 請求項 19 または 20 に記載のホストサーバであって、インターネットもしくは電話網を通じて携帯電話機と通信する手段を備え、自身が異常を検知した場合におけるその旨やその内容、もしくは、前記セキュリティ管理サーバから送られてくる前記異常を検知した旨やその内容を、音声通話もしくは電子メールにより所定の携帯電話機に通報する手段を備えることを特徴とする。

【請求項 22】 請求項 17～21 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機との間で通信する手段と、所定の携帯電話機から送られてくる前記通信関連情報についての問い合わせメッセージを受信する手段と、前記問い合わせメッセージに対応する前記通信関連情報を、記憶管理している前記通信関連情報から検索する手段と、その検索結果を記載したメッセージを前記携帯電話機に送信する手段と、を備えることを特徴とする。

【請求項 23】 請求項 17～22 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機と通信する手段と、

所定の携帯電話機から送られてくる前記監視対象装置を特定する情報およびその装置で実行される処理コマンドを受信する手段と、

前記処理コマンドをインターネットを通じて前記特定情報で特定される装置に送信する手段と、

前記装置から送られてくる前記処理コマンドの実行結果を受信して、その実行結果を前記携帯電話機のユーザインターフェースに適した形態の映像に編成し、これを前記携帯電話機に送信する手段を備えることを特徴とする。

【請求項 24】 請求項 1～23 のいずれかに記載のセキュリティ管理サーバであって、前記通信関連情報が前記 LAN を流れる通信パケットであり、前記通信パケットを収集する手段を備えることを特徴とする。



【請求項 2 5】 請求項 2 4 に記載のセキュリティ管理サーバであって、当該セキュリティ管理サーバ自身が前記 LAN を通じて直接前記通信パケットを取得する手段を備えることを特徴とする。

【請求項 2 6】 請求項 2 4 または 2 5 に記載のセキュリティ管理サーバであって、前記 LAN 内で稼働する前記監視対象装置により取得され前記監視対象装置に記憶管理されている通信パケットを前記 LAN を通じて集信する手段を備えることを特徴とする。

【請求項 2 7】 請求項 2 4 ～ 2 6 のいずれかに記載のセキュリティ管理サーバであって、

前記通信パケットに基づいて、前記監視対象装置の台数やこの台数を所定のグループ別に集計した値、前記監視対象装置が前記 LAN を通じて送受信した通信パケット数、およびこの通信パケット数を所定のグループ別に集計した値、の少なくとも一部を算出する手段を備え、

算出された前記各値の少なくとも一部の値を視覚的に表現した映像を生成し、その映像を前記 LAN を通じて接続する前記監視装置に送信する手段を備えることを特徴とする。

【請求項 2 8】 請求項 2 4 ～ 2 7 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置に対するアクセス制限情報を記憶管理する手段と、

前記通信パケットに基づいて前記アクセス制限情報に反する権限外アクセスを監視する手段と、

前記権限外アクセスを認知した場合にその旨を視覚的に表現した映像を生成し前記映像を前記監視装置に送信する手段とを備えることを特徴とする。

【請求項 2 9】 請求項 2 4 ～ 2 8 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置上で運用されるシステムごとのアクセス許可情報を記憶管理する手段と、

前記通信パケットに基づいて前記アクセス許可情報に反する権限外アクセスを監視する手段と、

前記アクセス許可情報に反するアクセスを認知した場合にその旨を表現した映像を生成する手段と、

前記映像を前記監視装置に送信する手段とを備えることを特徴とする。

【請求項 3 0】 請求項 2 4 ～ 2 9 のいずれかに記載のセキュリティ管理サーバであって、

前記通信パケットに基づいて前記各監視対象装置間で行われる通信や前記各監視対象装置のユーザのアクセス状況、前記各監視対象装置で動作するデータベースへの前記各監視対象装置もしくはユーザからのアクセス状況を視覚化した映像を、前記 LAN 内で稼働する各装置の抽象図案を前記各装置の現実の配置状態に則した形態に配置した映像に重ねて描画した映像を生成し、

前記映像を前記監視装置に送信する手段を備えることを特徴とする。

【請求項 3 1】 請求項 2 4 ～ 3 0 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置を利用するユーザごとの前記監視対象装置の利用履歴を前記通信パケットに基づいて検知し、前記利用履歴を記載した映像を前記監視装置に送信する手段を備えることを特徴とする。

【請求項 3 2】 請求項 2 4 ～ 3 1 のいずれかに記載のセキュリティ管理サーバであって、

前記通信パケットに基づいて調べた前記監視対象装置で送受信される通信パケットの数を前記監視対象装置上で運用されるシステムごとに集計する手段と、

その集計値を前記システムごとに視覚化した映像を生成する手段と、

前記映像を前記監視装置に送信する手段と、を備えることを特徴とする。

【請求項 3 3】 請求項 2 4 ～ 3 2 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置の稼働状態を前記通信パケットに基づいて調べる手段と、

前記各監視対象装置の稼働状態を前記監視対象装置を用いて運用されるシステム別に分類して視覚化した映像を生成する手段と、

前記映像を前記監視装置に送信する手段と、を備えることを特徴とする。

【請求項 3 4】 請求項 2 4 ～ 3 3 のいずれかに記載のセキュリティ管理サ

サーバであって、

前記監視対象装置で運用されるデータベースへのアクセス頻度を前記通信パケットに基づいて検知する手段と、

前記監視対象装置別もしくは前記監視対象装置を利用して運用されるシステム別に分類して視覚化した映像を生成する手段と、

前記映像を前記監視装置に送信する手段と、を備えることを特徴とする。

【請求項 3 5】 請求項 1 ～ 3 4 のいずれかに記載のセキュリティ管理サーバであって、

前記監視対象装置において蓄積記録されている当該監視対象装置におけるプログラムの実行履歴を前記 LAN を通じて収集する手段と、

前記実行履歴に基づいて前記監視対象装置におけるプログラムの実行履歴を視覚化した映像を生成する手段と、

前記映像を前記監視装置に送信する手段と、を備えることを特徴とする。

【請求項 3 6】 インターネットなどの外部のネットワークに接続する LAN 内に設置され、

前記 LAN 内で稼働する装置で記憶管理されているログ情報を受動的もしくは能動的に収集する手段と、

収集した前記ログ情報から前記 LAN でのセキュリティ管理に有用な情報を抽出しその情報を所定の形態に視覚化した映像を生成する手段と、

前記映像を前記 LAN を通じて能動的もしくは受動的に他の装置に送信する手段と、

を備えることを特徴とするセキュリティ管理サーバ。

【請求項 3 7】 請求項 3 6 に記載のセキュリティ管理サーバであって、収集した前記ログ情報に基づいて前記 LAN 内で稼働する装置のセキュリティ上の異常を検知する手段と、その異常を検知した場合にその旨やその内容を前記映像に反映させる手段と、を備えることを特徴とする。

【請求項 3 8】 請求項 3 6 または 3 7 に記載のセキュリティ管理サーバであって、

前記映像を生成する手段が、

前記LAN内で稼働する前記装置と、これと通信する前記外部のネットワークで稼働する装置と、これら装置を利用中のユーザと、前記LAN内外の各装置間で行われる通信とを、それぞれ所定のオブジェクトに視覚化した映像を生成する手段を備えることを特徴とする。

【請求項39】 請求項38に記載のセキュリティ管理サーバであって、

前記映像を生成する手段が、

前記各オブジェクトを所定の基準に従ってグループ分けし、各グループ別に階層的に視覚化した映像を生成する手段を備えることを特徴とする。

【請求項40】 請求項39に記載のセキュリティ管理サーバであって、前記基準が、各種装置と前記LANとの間の信頼度に基づくものであることを特徴とする。

【請求項41】 請求項36～40のいずれかに記載のセキュリティ管理サーバであって、

前記映像を生成する手段が、

前記各装置において行われた各種の処理がその内容と実行日時とを含むテキストメッセージの形式で行別記載されて構成されるログ情報に基づいて、テキストメッセージをそのまま表示するエリアと、所定の文字列の前記ログ情報中における出現頻度をグラフ表示したエリアと、前記文字列の所定単位期間ごとの出現頻度を時系列的にグラフ表示したエリアと、前記テキストメッセージの各行の長さをグラフ表示したエリアと、を備えて構成される映像を生成する機能を備えることを特徴とする。

【請求項42】 請求項36～41のいずれかに記載のセキュリティ管理サーバであって、

前記LAN内で稼働する前記装置が、

前記ログ情報の実体であるログファイルを、正本ファイルと、これとリアルタイムに同一内容に維持管理された複数の副本ファイルとの複数立てで管理し、前記各ファイルを当該装置内の記憶手段に適宜に区画された複数の記憶場所に分散して記憶管理する手段と、前記各副本ファイルを他の前記記憶場所に適宜移送する手段と、前記正副両ログファイルにセキュリティ上の異常がないかどうかを検

知する手段と、異常を検知した場合にその旨やその内容を前記セキュリティ管理サーバに通知する手段とを有し、

前記映像を生成する手段が、前記装置から通知される、前記異常を検知した旨やその内容を、前記映像に反映させる手段を備えることを特徴とする。

【請求項 4 3】 請求項 3 6～4 2 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータから送られてくる更新データを受信する手段と、前記映像を生成する手段を提供するソフトウェアの内容を前記更新データにより更新する手段とを備えることを特徴とする。

【請求項 4 4】 請求項 3 6～4 3 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報をこのコンピュータとの間で能動的もしくは受動的に送受信する手段を備えることを特徴とする。

【請求項 4 5】 請求項 3 6～4 4 のいずれかに記載のセキュリティ管理サーバであって、前記ログ情報の収集対象となる前記 LAN 内で稼働する前記装置についての情報や、前記映像を生成する手段で利用・参照される情報などの各種の設定登録情報を記憶管理する手段を備え、

前記外部のネットワークで稼働する所定のコンピュータと通信し、前記設定登録情報を前記コンピュータとの間で能動的もしくは受動的に送受信する手段を備えることを特徴とする。

【請求項 4 6】 請求項 3 6～4 5 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報や当該セキュリティ管理サーバ自身が記憶管理している自身のログ情報に基づいて、前記装置や当該セキュリティ管理サーバ自身のセキュリティ上の異常を検知する手段と、

異常を検知した場合にその旨やその内容を、前記コンピュータとの間で能動的もしくは受動的に送受信する手段を備えることを特徴とする。

【請求項 4 7】 請求項 3 6～4 6 のいずれかに記載のセキュリティ管理サーバであって、

前記 LAN 内の各装置との間で TCP / IP プロトコルに基づいて通信する手段と、

前記 LAN 内の前記装置からの要求に応じて所定の IP アドレスを割り当てるとともにその IP アドレスと前記装置の MAC アドレスとの対応づけの履歴を記載した割当履歴を記憶管理する手段と、

収集した前記ログ情報をそれがどの装置についてのログ情報であるかを特定する IP アドレスを付帯させて記憶管理する手段と、

前記割当履歴において同一の MAC アドレスに対応づけられた IP アドレスが付帯する前記ログ情報を、同一の装置についてのログ情報であるとして取り扱う手段と、

を備えることを特徴とする。

【請求項 4 8】 請求項 4 7 に記載のセキュリティ管理サーバであって、前記 LAN 内で稼働する他のセキュリティ管理サーバとの間で前記割当履歴を相互に送受信する手段と、

受信した他のセキュリティ管理サーバにおける前記割当履歴と、自身が記憶管理している前記割当履歴とを統合管理し、これら割当履歴において同一の MAC アドレスに対応づけられた IP アドレスが付帯する前記ログ情報を、同一の装置についてのログ情報であるとして取り扱う手段と、

を備えることを特徴とする。

【請求項 4 9】 請求項 4 7 または 4 8 に記載のセキュリティ管理サーバであって、前記割当履歴に対応づけて記述される MAC アドレスと IP アドレスの各組み合わせにはその IP アドレスの有効期間情報が付帯し、この有効期間情報と収集した前記ログ情報に付帯して記録されている当該ログ情報の生成日時とを比較して、前記生成日時において前記ログ情報に付帯する IP アドレスが対応づけされていた MAC アドレスを特定する手段を備えることを特徴とする。

【請求項 5 0】 請求項 4 3 における前記所定のコンピュータとして機能するホストサーバであって、前記更新データを適宜前記セキュリティ管理サーバに送信する手段を備えることを特徴とする。

【請求項 5 1】 請求項 4 4 における前記所定のコンピュータとして機能す

るホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記ログ情報を記憶管理する手段を備えることを特徴とする。

【請求項 5 2】 請求項 5 1 に記載の前記ホストサーバであって、記憶管理している前記ログ情報を能動的もしくは受動的に前記セキュリティ管理サーバに送信する手段を備えることを特徴とする。

【請求項 5 3】 請求項 5 1 または 5 2 に記載のホストサーバであって、記憶管理している前記ログ情報に基づいて前記 LAN 内の装置にセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を該当の LAN 内に設置されたセキュリティ管理サーバに送信する手段を備えることを特徴とする。

【請求項 5 4】 請求項 5 1 ～ 5 3 のいずれかに記載のホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記各種設定情報、もしくは、前記異常を検知した旨やその内容を、能動的もしくは受動的に受信してこれを記憶管理する手段を備えることを特徴とする。

【請求項 5 5】 請求項 5 3 または 5 4 に記載のホストサーバであって、インターネットもしくは電話網を通じて携帯電話機と通信する手段を備え、自身が異常を検知した場合におけるその旨やその内容、もしくは、前記セキュリティ管理サーバから送られてくる前記異常を検知した旨やその内容を、音声通話もしくは電子メールにより所定の携帯電話機に通報する手段を備えることを特徴とする。

【請求項 5 6】 請求項 5 1 ～ 5 5 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機との間で通信する手段と、所定の携帯電話機から送られてくる前記ログ情報についての問い合わせメッセージを受信する手段と、前記問い合わせメッセージに対応する前記ログ情報を、記憶管理している前記ログ情報から検索する手段と、その検索結果を記載したメッセージを前記携帯電話機に送信する手段と、を備えることを特徴とする。

【請求項 5 7】 請求項 5 1 ～ 5 6 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機と通信する手段と、

所定の携帯電話機から送られてくる前記 LAN 内で稼働する装置を特定する情

報およびその装置で実行される処理コマンドを受信する手段と、

前記処理コマンドをインターネットを通じて前記特定情報で特定される装置に送信する手段と、

前記装置から送られてくる前記処理コマンドの実行結果を受信して、その実行結果を前記携帯電話機のユーザインターフェースに適した形態の映像に編成し、これを前記携帯電話機に送信する手段を備えることを特徴とする。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、インターネットなどの外部のネットワークと接続するLAN内に設置され、このLANにおけるセキュリティサービスを提供するセキュリティ管理サーバ、およびこのセキュリティ管理サーバと連携して動作するホストサーバに関し、LANにおけるセキュリティ管理に有用な各種のサービスを提供する技術に関する。

【0002】

【従来の技術】

一般に、会社などの組織に閉域的に敷設されるいわゆるLANは、電子メールの交換や、宣伝広告・電子商取引などを目的としたWebページの公開などの必要のため、インターネットなどの外部のネットワークと接続する形態で運用されていることが多い。ここでこのような形で運用されるLANのセキュリティ管理は、ルータ設定の工夫やファイアウォールの構築により行われるのが普通である。

【0003】

しかしながら、例えば、出先の社員からの社内のコンピュータにアクセスを許可せざるを得ない場合のように、セキュリティは常に利便性と背中合わせであり、ルータの設定やファイアウォールによるのみでは、外部ネットワークからの不正侵入を完全に防御することはできない。また、これらはいわゆる内部者の不正行為に対しては無力である。

【0004】

一方、よく知られているように、セキュリティ管理にはLAN内の各種装置に



記憶管理されている履歴情報、いわゆるログ情報がよく利用されており、ログ情報には、外部ネットワークからのアクセス履歴などのセキュリティ管理に有用な情報が多く含まれているため、これを調査・分析することで、例えば、不正行為がどのようにして行われたか、対象は何か、どこからの侵入者か、被害を受けたファイルやデータはどれか、といったことを詳細に把握することができる。従って、不正行為の事後的な追跡調査においてログ情報は非常に有効である。

#### 【0005】

##### 【発明が解決しようとする課題】

しかしながら、一般にログ情報に含まれる情報は膨大で、その解析作業には相当の労力が必要となる。また、これを解析して有用な情報を抽出するにはそれなりの技術や経験を要し、有用な情報が含まれていても必ずしも十分に利用されていないことも多い。さらに、LAN内に多くの装置が稼働している場合には、各装置内から必要なログ情報の収集も大変面倒である。

#### 【0006】

一方、不正行為の監視や事後的な調査は、ログ情報だけでなくLAN上を流れる通信パケットを利用して行うこともできるが、一般にLAN上を流れる通信パケットの量は膨大であり、通信パケットを利用して不正行為の監視等を行う場合にもやはりそれなりの熟練や知識が要求される。

#### 【0007】

この発明はこのような事情に鑑みてなされたもので、ログ情報や通信パケットから得られる、監視対象装置のセキュリティ管理に有用な情報を、ユーザが利用しやすい形で提供することができる、セキュリティサービスを提供するサーバ装置およびこれと連携して動作するホストサーバを提供することを目的とする。

#### 【0008】

##### 【課題を解決するための手段】

この目的を達成するための本発明の請求項1に記載の発明は、セキュリティ管理サーバであって、所定のLAN内に設置され、前記LAN内で稼働する監視対象装置が前記LANを通じて行う通信に関連する情報を収集する手段と、収集した前記通信関連情報から前記LANにおけるセキュリティ管理に有用な情報を抽

出しその情報を所定の形態に視覚化した映像を生成する手段と、前記映像を監視装置に送信する手段と、を備えることとする。

## 【 0 0 0 9 】

また、本発明の請求項 2 に記載の発明は、請求項 1 に記載のセキュリティ管理サーバであって、前記通信関連情報に基づいて前記監視対象装置のセキュリティ上の異常を検知する手段と、その異常を検知した場合にその旨やその内容を前記映像に反映させる手段と、を備えることとする。

## 【 0 0 1 0 】

また、本発明の請求項 3 に記載の発明は、請求項 1 または 2 に記載のセキュリティ管理サーバであって、前記通信関連情報が前記監視対象装置に記憶管理されているログ情報であり、前記ログ情報を前記 LAN を通じて収集する手段を備えることとする。

## 【 0 0 1 1 】

また、本発明の請求項 4 に記載の発明は、請求項 1 ～ 3 のいずれかに記載のセキュリティ管理サーバであって、前記 LAN がインターネットなどの外部のネットワークにも接続し、前記映像を生成する手段が、前記監視対象装置と、これと通信する前記外部のネットワークで稼働する装置と、これらの装置を利用中のユーザと、前記 LAN 内外の各装置間で行われる通信とを、それぞれ所定のオブジェクトに視覚化した映像を生成する手段を備えることとする。

## 【 0 0 1 2 】

また、本発明の請求項 5 に記載の発明は、請求項 4 に記載のセキュリティ管理サーバであって、前記映像を生成する手段が、前記各オブジェクトを所定の基準に従ってグループ分けし、各グループ別に階層的に視覚化した映像を生成する手段を備えることとする。

## 【 0 0 1 3 】

また、本発明の請求項 6 に記載の発明は、請求項 5 に記載のセキュリティ管理サーバであって、前記基準が、前記各装置と前記 LAN との間の信頼度に基づくものであることとする。

## 【 0 0 1 4 】

また、本発明の請求項 7 に記載の発明は、請求項 3 ～ 6 のいずれかに記載のセキュリティ管理サーバであって、前記映像を生成する手段が、前記各監視対象装置において行われた各種の処理がその内容と実行日時とを含むテキストメッセージの形式で行別記載されて構成されるログ情報に基づいて、テキストメッセージをそのまま表示するエリアと、所定の文字列の前記ログ情報中における出現頻度をグラフ表示したエリアと、前記文字列の所定単位期間ごとの出現頻度を時系列的にグラフ表示したエリアと、前記テキストメッセージの各行の長さをグラフ表示したエリアと、を備えて構成される映像を生成する機能を備えることとする。

## 【 0 0 1 5 】

また、本発明の請求項 8 に記載の発明は、請求項 3 ～ 7 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置が、前記ログ情報の実体であるログファイルを、正本ファイルと、これとリアルタイムに同一内容に維持管理された複数の副本ファイルとの複数立てで管理し、前記各ファイルを当該監視対象装置内の記憶手段に適宜に区画された複数の記憶場所に分散して記憶管理する手段と、前記各副本ファイルを他の前記記憶場所に適宜移送する手段と、前記正副両ログファイルにセキュリティ上の異常がないかどうかを検知する手段と、異常を検知した場合にその旨やその内容を前記セキュリティ管理サーバに通知する手段とを有し、前記映像を生成する手段が、前記監視対象装置から通知される、前記異常を検知した旨やその内容を、前記映像に反映させる手段を備えることとする。

## 【 0 0 1 6 】

また、本発明の請求項 9 に記載の発明は、請求項 4 ～ 8 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータから送られてくる更新データを受信する手段と、前記映像を生成する手段を提供するソフトウェアの内容を前記更新データにより更新する手段とを備えることとする。

## 【 0 0 1 7 】

また、本発明の請求項 1 0 に記載の発明は、請求項 4 ～ 9 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコ

ンピュータと通信し、収集した前記ログ情報をこのコンピュータとの間で送受信する手段を備えることとする。

## 【 0 0 1 8 】

また、本発明の請求項 1 1 に記載の発明は、請求項 4 ～ 1 0 のいずれかに記載のセキュリティ管理サーバであって、前記ログ情報の収集対象となる前記監視対象装置についての情報や、前記映像を生成する手段で利用・参照される情報などの各種の設定登録情報を記憶管理する手段を備え、前記外部のネットワークで稼働する所定のコンピュータと通信し、前記設定登録情報を前記コンピュータとの間で送受信する手段を備えることとする。

## 【 0 0 1 9 】

また、本発明の請求項 1 2 に記載の発明は、請求項 4 ～ 1 1 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報や当該セキュリティ管理サーバ自身が記憶管理している自身のログ情報に基づいて、前記監視対象装置や当該セキュリティ管理サーバ自身のセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を、前記コンピュータとの間で送受信する手段を備えることとする。

## 【 0 0 2 0 】

また、本発明の請求項 1 3 に記載の発明は、請求項 1 ～ 1 2 のいずれかに記載のセキュリティ管理サーバであって、前記各監視対象装置との間で T C P / I P プロトコルに基づいて通信する手段と、前記 L A N 内の前記各監視対象装置からの要求に応じて所定の I P アドレスを割り当てるとともにその I P アドレスと前記各監視対象装置の M A C アドレスとの対応づけの履歴を記載した割当履歴を記憶管理する手段と、収集した前記通信関連情報をそれがどの前記監視対象装置に関する通信関連情報であるかを特定する I P アドレスを付帯させて記憶管理する手段と、前記割当履歴において同一の M A C アドレスに対応づけられた I P アドレスが付帯する前記通信関連情報を、同一の前記監視対象装置に関する通信関連情報であるとして取り扱う手段と、を備えることとする。

## 【 0 0 2 1 】

また、本発明の請求項 1 4 に記載の発明は、請求項 1 3 に記載のセキュリティ管理サーバであって、前記 LAN 内で稼働する他のセキュリティ管理サーバとの間で前記割当履歴を相互に送受信する手段と、受信した他のセキュリティ管理サーバにおける前記割当履歴と、自身が記憶管理している前記割当履歴とを統合管理し、これら割当履歴において同一の MAC アドレスに対応づけられた IP アドレスが付帯する前記通信関連情報を、同一の前記監視対象装置に関する通信関連情報であるとして取り扱う手段と、を備えることとする。

## 【 0 0 2 2 】

また、本発明の請求項 1 5 に記載の発明は、請求項 1 3 または 1 4 に記載のセキュリティ管理サーバであって、前記割当履歴に対応づけて記述される MAC アドレスと IP アドレスの各組み合わせにはその IP アドレスの有効期間情報が付帯し、この有効期間情報と収集した前記通信関連情報に付帯して記録されている当該通信関連情報の生成日時とを比較して、前記生成日時において前記通信関連情報に付帯する IP アドレスが対応づけされていた MAC アドレスを特定する手段を備えることとする。

## 【 0 0 2 3 】

また、本発明の請求項 1 6 に記載の発明は、請求項 9 における前記所定のコンピュータとして機能するホストサーバであって、前記更新データを適宜前記セキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 2 4 】

また、本発明の請求項 1 7 に記載の発明は、請求項 1 0 における前記所定のコンピュータとして機能するホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記通信関連情報を記憶管理する手段を備えることとする。

## 【 0 0 2 5 】

また、本発明の請求項 1 8 に記載の発明は、請求項 1 7 に記載の前記ホストサーバであって、記憶管理している前記通信関連情報を前記セキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 2 6 】

また、本発明の請求項 1 9 に記載の発明は、請求項 1 7 または 1 8 に記載の前

記ホストサーバであって、記憶管理している前記通信関連情報に基づいて前記監視対象装置についてのセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を該当のLAN内に設置されたセキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 2 7 】

また、本発明の請求項 2 0 に記載の発明は、請求項 1 7 ～ 1 9 のいずれかに記載のホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記各種設定情報、もしくは、前記異常を検知した旨やその内容を受信してこれを記憶管理する手段を備えることとする。

## 【 0 0 2 8 】

また、本発明の請求項 2 1 に記載の発明は、請求項 1 9 または 2 0 に記載のホストサーバであって、インターネットもしくは電話網を通じて携帯電話機と通信する手段を備え、自身が異常を検知した場合におけるその旨やその内容、もしくは、前記セキュリティ管理サーバから送られてくる前記異常を検知した旨やその内容を、音声通話もしくは電子メールにより所定の携帯電話機に通報する手段を備えることとする。

## 【 0 0 2 9 】

また、本発明の請求項 2 2 に記載の発明は、請求項 1 7 ～ 2 1 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機との間で通信する手段と、所定の携帯電話機から送られてくる前記通信関連情報についての問い合わせメッセージを受信する手段と、前記問い合わせメッセージに対応する前記通信関連情報を、記憶管理している前記通信関連情報から検索する手段と、その検索結果を記載したメッセージを前記携帯電話機に送信する手段と、を備えることとする。

## 【 0 0 3 0 】

また、本発明の請求項 2 3 に記載の発明は、請求項 1 7 ～ 2 2 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機と通信する手段と、所定の携帯電話機から送られてくる前記監視対象装置を特定する情報およびその装置で実行される処理コマンドを受信する手段と、前記処理コマンドをイン

ターネットを通じて前記特定情報で特定される装置に送信する手段と、前記装置から送られてくる前記処理コマンドの実行結果を受信して、その実行結果を前記携帯電話機のユーザインターフェースに適した形態の映像に編成し、これを前記携帯電話機に送信する手段を備えることとする。

## 【 0 0 3 1 】

また、本発明の請求項 2 4 に記載の発明は、請求項 1 ～ 2 3 のいずれかに記載のセキュリティ管理サーバであって、前記通信関連情報が前記 LAN を流れる通信パケットであり、前記通信パケットを収集する手段を備えることとする。

## 【 0 0 3 2 】

また、本発明の請求項 2 5 に記載の発明は、請求項 2 4 に記載のセキュリティ管理サーバであって、当該セキュリティ管理サーバ自身が前記 LAN を通じて直接前記通信パケットを取得する手段を備えることとする。

## 【 0 0 3 3 】

また、本発明の請求項 2 6 に記載の発明は、請求項 2 4 または 2 5 に記載のセキュリティ管理サーバであって、前記 LAN 内で稼働する前記監視対象装置により取得され前記監視対象装置に記憶管理されている通信パケットを前記 LAN を通じて集信する手段を備えることとする。

## 【 0 0 3 4 】

また、本発明の請求項 2 7 に記載の発明は、請求項 2 4 ～ 2 6 のいずれかに記載のセキュリティ管理サーバであって、前記通信パケットに基づいて、前記監視対象装置の台数やこの台数を所定のグループ別に集計した値、前記監視対象装置が前記 LAN を通じて送受信した通信パケット数、およびこの通信パケット数を所定のグループ別に集計した値、の少なくとも一部を算出する手段を備え、算出された前記各値の少なくとも一部の値を視覚的に表現した映像を生成し、その映像を前記 LAN を通じて接続する前記監視装置に送信する手段を備えることとする。

## 【 0 0 3 5 】

また、本発明の請求項 2 8 に記載の発明は、請求項 2 4 ～ 2 7 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置に対するアクセス制限

情報を記憶管理する手段と、前記通信パケットに基づいて前記アクセス制限情報に反する権限外アクセスを監視する手段と、前記権限外アクセスを認知した場合にその旨を視覚的に表現した映像を生成し前記映像を前記監視装置に送信する手段とを備えることとする。

## 【 0 0 3 6 】

また、本発明の請求項 2 9 に記載の発明は、請求項 2 4 ～ 2 8 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置上で運用されるシステムごとのアクセス許可情報を記憶管理する手段と、前記通信パケットに基づいて前記アクセス許可情報に反する権限外アクセスを監視する手段と、前記アクセス許可情報に反するアクセスを認知した場合にその旨を表現した映像を生成する手段と、前記映像を前記監視装置に送信する手段とを備えることとする。

## 【 0 0 3 7 】

また、本発明の請求項 3 0 に記載の発明は、請求項 2 4 ～ 2 9 のいずれかに記載のセキュリティ管理サーバであって、前記通信パケットに基づいて前記各監視対象装置間で行われる通信や前記各監視対象装置のユーザのアクセス状況、前記各監視対象装置で動作するデータベースへの前記各監視対象装置もしくはユーザからのアクセス状況を視覚化した映像を、前記 LAN 内で稼働する各装置の抽象図案を前記各装置の現実の配置状態に則した形態に配置した映像に重ねて描画した映像を生成し、前記映像を前記監視装置に送信する手段を備えることとする。

## 【 0 0 3 8 】

また、本発明の請求項 3 1 に記載の発明は、請求項 2 4 ～ 3 0 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置を利用するユーザごとの前記監視対象装置の利用履歴を前記通信パケットに基づいて検知し、前記利用履歴を記載した映像を前記監視装置に送信する手段を備えることとする。

## 【 0 0 3 9 】

また、本発明の請求項 3 2 に記載の発明は、請求項 2 4 ～ 3 1 のいずれかに記載のセキュリティ管理サーバであって、前記通信パケットに基づいて調べた前記監視対象装置で送受信される通信パケットの数を前記監視対象装置上で運用されるシステムごとに集計する手段と、その集計値を前記システムごとに視覚化した



映像を生成する手段と、前記映像を前記監視装置に送信する手段と、を備えることとする。

## 【 0 0 4 0 】

また、本発明の請求項 3 3 に記載の発明は、請求項 2 4 ～ 3 2 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置の稼働状態を前記通信パケットに基づいて調べる手段と、前記各監視対象装置の稼働状態を前記監視対象装置を用いて運用されるシステム別に分類して視覚化した映像を生成する手段と、前記映像を前記監視装置に送信する手段と、を備えることを特徴とする。

## 【 0 0 4 1 】

また、本発明の請求項 3 4 に記載の発明は、請求項 2 4 ～ 3 3 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置で運用されるデータベースへのアクセス頻度を前記通信パケットに基づいて検知する手段と、前記監視対象装置別もしくは前記監視対象装置を利用して運用されるシステム別に分類して視覚化した映像を生成する手段と、前記映像を前記監視装置に送信する手段と、を備えることとする。

## 【 0 0 4 2 】

また、本発明の請求項 3 5 に記載の発明は、請求項 1 ～ 3 4 のいずれかに記載のセキュリティ管理サーバであって、前記監視対象装置において蓄積記録されている当該監視対象装置におけるプログラムの実行履歴を前記 LAN を通じて収集する手段と、前記実行履歴に基づいて前記監視対象装置におけるプログラムの実行履歴を視覚化した映像を生成する手段と、前記映像を前記監視装置に送信する手段と、を備えることとする。

## 【 0 0 4 3 】

また、本発明の請求項 3 6 に記載の発明は、インターネットなどの外部のネットワークに接続する LAN 内に設置され、前記 LAN 内で稼働する装置で記憶管理されているログ情報を受動的もしくは能動的に収集する手段と、収集した前記ログ情報から前記 LAN でのセキュリティ管理に有用な情報を抽出しその情報を所定の形態に視覚化した映像を生成する手段と、前記映像を前記 LAN を通じて能動的もしくは受動的に他の装置に送信する手段と、を備えることとする。

## 【 0 0 4 4 】

また、本発明の請求項 3 7 に記載の発明は、請求項 3 6 に記載のセキュリティ管理サーバであって、収集した前記ログ情報に基づいて前記 LAN 内で稼働する装置のセキュリティ上の異常を検知する手段と、その異常を検知した場合にその旨やその内容を前記映像に反映させる手段と、を備えることとする。

## 【 0 0 4 5 】

また、本発明の請求項 3 8 に記載の発明は、請求項 3 6 または 3 7 に記載のセキュリティ管理サーバであって、前記映像を生成する手段が、前記 LAN 内で稼働する前記装置と、これと通信する前記外部のネットワークで稼働する装置と、これら装置を利用中のユーザと、前記 LAN 内外の各装置間で行われる通信とを、それぞれ所定のオブジェクトに視覚化した映像を生成する手段を備えることとする。

## 【 0 0 4 6 】

また、本発明の請求項 3 9 に記載の発明は、請求項 3 8 に記載のセキュリティ管理サーバであって、前記映像を生成する手段が、前記各オブジェクトを所定の基準に従ってグループ分けし、各グループ別に階層的に視覚化した映像を生成する手段を備えることとする。

## 【 0 0 4 7 】

また、本発明の請求項 4 0 に記載の発明は、請求項 3 9 に記載のセキュリティ管理サーバであって、前記基準が、各種装置と前記 LAN との間の信頼度に基づくものであることとする。

## 【 0 0 4 8 】

また、本発明の請求項 4 1 に記載の発明は、請求項 3 6 ～ 4 0 のいずれかに記載のセキュリティ管理サーバであって、前記映像を生成する手段が、前記各装置において行われた各種の処理がその内容と実行日時とを含むテキストメッセージの形式で行別記載されて構成されるログ情報に基づいて、テキストメッセージをそのまま表示するエリアと、所定の文字列の前記ログ情報中における出現頻度をグラフ表示したエリアと、前記文字列の所定単位期間ごとの出現頻度を時系列的にグラフ表示したエリアと、前記テキストメッセージの各行の長さをグラフ表示

したエリアと、を備えて構成される映像を生成する機能を備えることとする。

【0049】

また、本発明の請求項42に記載の発明は、請求項36～41のいずれかに記載のセキュリティ管理サーバであって、前記LAN内で稼働する前記装置が、前記ログ情報の実体であるログファイルを、正本ファイルと、これとリアルタイムに同一内容に維持管理された複数の副本ファイルとの複数立てで管理し、前記各ファイルを当該装置内の記憶手段に適宜に区画された複数の記憶場所に分散して記憶管理する手段と、前記各副本ファイルを他の前記記憶場所に適宜移送する手段と、前記正副両ログファイルにセキュリティ上の異常がないかどうかを検知する手段と、異常を検知した場合にその旨やその内容を前記セキュリティ管理サーバに通知する手段とを有し、前記映像を生成する手段が、前記装置から通知される、前記異常を検知した旨やその内容を、前記映像に反映させる手段を備えることとする。

【0050】

また、本発明の請求項43に記載の発明は、請求項36～42のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータから送られてくる更新データを受信する手段と、前記映像を生成する手段を提供するソフトウェアの内容を前記更新データにより更新する手段とを備えることとする。

【0051】

また、本発明の請求項44に記載の発明は、請求項36～43のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報をこのコンピュータとの間で能動的もしくは受動的に送受信する手段を備えることとする。

【0052】

また、本発明の請求項45に記載の発明は、請求項36～44のいずれかに記載のセキュリティ管理サーバであって、前記ログ情報の収集対象となる前記LAN内で稼働する前記装置についての情報や、前記映像を生成する手段で利用・参照される情報などの各種の設定登録情報を記憶管理する手段を備え、前記外部の

ネットワークで稼働する所定のコンピュータと通信し、前記設定登録情報を前記コンピュータとの間で能動的もしくは受動的に送受信する手段を備えることとする。

## 【 0 0 5 3 】

また、本発明の請求項 4 6 に記載の発明は、請求項 3 6 ～ 4 5 のいずれかに記載のセキュリティ管理サーバであって、前記外部のネットワークで稼働する所定のコンピュータと通信し、収集した前記ログ情報や当該セキュリティ管理サーバ自身が記憶管理している自身のログ情報に基づいて、前記装置や当該セキュリティ管理サーバ自身のセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を、前記コンピュータとの間で能動的もしくは受動的に送受信する手段を備えることとする。

## 【 0 0 5 4 】

また、本発明の請求項 4 7 に記載の発明は、請求項 3 6 ～ 4 6 のいずれかに記載のセキュリティ管理サーバであって、前記 LAN 内の各装置との間で TCP / IP プロトコルに基づいて通信する手段と、前記 LAN 内の前記装置からの要求に応じて所定の IP アドレスを割り当てるとともにその IP アドレスと前記装置の MAC アドレスとの対応づけの履歴を記載した割当履歴を記憶管理する手段と、収集した前記ログ情報をそれがどの装置についてのログ情報であるかを特定する IP アドレスを付帯させて記憶管理する手段と、前記割当履歴において同一の MAC アドレスに対応づけられた IP アドレスが付帯する前記ログ情報を、同一の装置についてのログ情報であるとして取り扱う手段と、を備えることとする。

## 【 0 0 5 5 】

また、本発明の請求項 4 8 に記載の発明は、請求項 4 7 に記載のセキュリティ管理サーバであって、前記 LAN 内で稼働する他のセキュリティ管理サーバとの間で前記割当履歴を相互に送受信する手段と、受信した他のセキュリティ管理サーバにおける前記割当履歴と、自身が記憶管理している前記割当履歴とを統合管理し、これら割当履歴において同一の MAC アドレスに対応づけられた IP アドレスが付帯する前記ログ情報を、同一の装置についてのログ情報であるとして取り扱う手段と、を備えることとする。

## 【 0 0 5 6 】

また、本発明の請求項 4 9 に記載の発明は、請求項 4 7 または 4 8 に記載のセキュリティ管理サーバであって、前記割当履歴に対応づけて記述される MAC アドレスと IP アドレスの各組み合わせにはその IP アドレスの有効期間情報が付帯し、この有効期間情報と収集した前記ログ情報に付帯して記録されている当該ログ情報の生成日時とを比較して、前記生成日時において前記ログ情報に付帯する IP アドレスが対応づけされていた MAC アドレスを特定する手段を備えることとする。

## 【 0 0 5 7 】

また、本発明の請求項 5 0 に記載の発明は、請求項 4 3 における前記所定のコンピュータとして機能するホストサーバであって、前記更新データを適宜前記セキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 5 8 】

また、本発明の請求項 5 1 に記載の発明は、請求項 4 4 における前記所定のコンピュータとして機能するホストサーバであって、前記セキュリティ管理サーバから送られてくる、前記ログ情報を記憶管理する手段を備えることとする。

## 【 0 0 5 9 】

また、本発明の請求項 5 2 に記載の発明は、請求項 5 1 に記載の前記ホストサーバであって、記憶管理している前記ログ情報を能動的もしくは受動的に前記セキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 6 0 】

また、本発明の請求項 5 3 に記載の発明は、請求項 5 1 または 5 2 に記載のホストサーバであって、記憶管理している前記ログ情報に基づいて前記 LAN 内の装置にセキュリティ上の異常を検知する手段と、異常を検知した場合にその旨やその内容を該当の LAN 内に設置されたセキュリティ管理サーバに送信する手段を備えることとする。

## 【 0 0 6 1 】

また、本発明の請求項 5 4 に記載の発明は、請求項 5 1 ～ 5 3 のいずれかに記載のホストサーバであって、前記セキュリティ管理サーバから送られてくる、前

記各種設定情報、もしくは、前記異常を検知した旨やその内容を、能動的もしくは受動的に受信してこれを記憶管理する手段を備えることとする。

## 【 0 0 6 2 】

また、本発明の請求項 5 5 に記載の発明は、請求項 5 3 または 5 4 に記載のホストサーバであって、インターネットもしくは電話網を通じて携帯電話機と通信する手段を備え、自身が異常を検知した場合におけるその旨やその内容、もしくは、前記セキュリティ管理サーバから送られてくる前記異常を検知した旨やその内容を、音声通話もしくは電子メールにより所定の携帯電話機に通報する手段を備えることとする。

## 【 0 0 6 3 】

また、本発明の請求項 5 6 に記載の発明は、請求項 5 1 ～ 5 5 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機との間で通信する手段と、所定の携帯電話機から送られてくる前記ログ情報についての問い合わせメッセージを受信する手段と、前記問い合わせメッセージに対応する前記ログ情報を、記憶管理している前記ログ情報から検索する手段と、その検索結果を記載したメッセージを前記携帯電話機に送信する手段と、を備えることとする。

## 【 0 0 6 4 】

また、本発明の請求項 5 7 に記載の発明は、請求項 5 1 ～ 5 6 のいずれかに記載のホストサーバであって、インターネットを通じて携帯電話機と通信する手段と、所定の携帯電話機から送られてくる前記 LAN 内で稼働する装置を特定する情報およびその装置で実行される処理コマンドを受信する手段と、前記処理コマンドをインターネットを通じて前記特定情報で特定される装置に送信する手段と、前記装置から送られてくる前記処理コマンドの実行結果を受信して、その実行結果を前記携帯電話機のユーザインターフェースに適した形態の映像に編成し、これを前記携帯電話機に送信する手段を備えることとする。

## 【 0 0 6 5 】

## 【発明の実施の形態】

図 1 は、本発明の一実施例によるセキュリティ管理サーバ S が設置された LAN の概略的なネットワーク構成図である。この LAN では、通信プロトコルの一

つとしてTCP/IPが採用され、外部ネットワークであるインターネットにも接続している。

## 【0066】

LAN内では、ルータなどのネットワーク機器、ファイアウォールサーバ、パソコンやオフコンなどの個人用パソコン、イントラネット用のWebサーバもしくはインターネット上のWebサーバとして機能するWebサーバ、インターネット上もしくはLAN内の電子メールの中継やユーザ管理を行うメールサーバ、DNSサーバ、各種のデータベースサーバ、グループウェアサーバなどのセキュリティ管理の対象となる各種の監視対象装置Cが稼働している。

## 【0067】

セキュリティ管理サーバSは、所定の事業者Aにより設置され運用されている。事業者Aは、LANを保有する会社などの組織と契約し、契約者のLAN内にセキュリティ管理サーバSを設置したり、後述するホストサーバHによる各種サービスの提供を業務として行っている。以下では、セキュリティ管理サーバS、ホストサーバHの機能について詳述する。

## 【0068】

===セキュリティ管理サーバの機能===

## &lt;バックアップサービス&gt;

セキュリティ管理サーバSは、バックアップサービス、すなわち、LAN内で稼働する各装置Cに格納されている各種のログ情報を収集して記憶管理する。ここでログ情報とは、例えば、監視対象となる装置Cで稼働するOSがUNIXである場合には、ログイン履歴情報が記録されている「wtmp」ログファイル、管理対象装置に対するアクセス履歴が記録されている「syslog」ファイル、ユーザIDを特権モード属性のユーザIDに一時的に変更するコマンドである「su」コマンドの実行履歴が記録される「sulog」ファイル、各種コマンドの実行履歴が記述された「pacct」ファイル、特定ファイルの属性変化が記録されたファイルなどである。

## 【0069】

セキュリティ管理サーバSには、ログ情報の収集の対象となる装置の特定情報

(例えば、ホスト名やIPアドレス)、ログ情報の格納場所(例えば、ログファイルが格納されているディレクトリ名やログファイルのファイル名)、収集するタイミングなどが登録されている。これらの登録情報は、当該セキュリティ管理サーバSが提供する登録用Webページなどを利用して登録や更新が行われる。

#### 【0070】

セキュリティ管理サーバSは、収集したログ情報を、ハードディスクなどに記憶管理する。これらログ情報は、後述する各種の処理に利用される他、例えば、不正アクセス等があった場合の追跡調査やログファイルが改竄・削除等された場合には、それらのバックアップファイルとして利用される。

#### 【0071】

#### <ログ情報の視覚化>

セキュリティ管理サーバSは、収集したログ情報から前記LANのセキュリティ管理に有用な情報を抽出し、これを人が利用しやすい形態に視覚化した映像を生成する。図2は視覚化された映像の一例であり、LAN内で稼働する各種の監視対象装置Cと、これらにアクセスしてくるLAN外部の装置と、LAN内外の装置にアクセスしているユーザと、これら装置の間で行われる通信とを、それぞれ所定のオブジェクトに三次元的に視覚化したものである。

#### 【0072】

この図において、外周円はルータなどで仕切られたLANなどの所定の概念で区分されたネットワークを示しており、この外周円上には、そのネットワーク内に存在する装置を表現した球オブジェクト11が描画される。一方、各外周円の内側に描かれている内周円部分には、前記ネットワーク内の装置を利用中のユーザを表現した立方体オブジェクト13が描画される。

#### 【0073】

この図において、球オブジェクト11と立方体オブジェクト13とを結ぶ線分オブジェクト15は、球オブジェクト11で表示された装置から、立方体オブジェクト13で表示されたユーザアカウント(ユーザID)を利用中(ログイン中)であることを示している。ここで線分オブジェクト15の種類(点線・実線等)は、例えば、その通信が遠隔操作のための通信であるとか、ファイル転送のた



めの通信であるとか、両方の方法によるアクセスである、といったその通信の形態を示している。なお、線分オブジェクト15には、例えば、この通信において実行されたコマンドなどが付記される場合もある。

## 【0074】

図2では、複数のネットワークが適宜に分類された信頼度に応じてグループ分けされ、各グループ別に階層的に視覚化して表示されている。この図では、セキュリティ管理サーバSが設置されているLANが最下層（すなわち、最も信頼できる）に表示され、他のネットワークはこのLANとの関係が疎遠なる程（信頼が薄くなる程）、上になるように表示され、最上層にはインターネットが表示されている。

## 【0075】

セキュリティ管理サーバSは、LAN内で稼働する監視対象装置Cから前記の映像の送出要求があると、その監視対象装置Cに対して前記映像を所定フォーマットの映像データとして送出する。すなわち、前記映像はLAN内で稼働する個人用パソコンなどの監視装置C（監視装置Cが同時に監視対象装置Cでもあるという場合もある）からWebブラウザや専用ツールなどを使って前記映像を適宜参照することができる。なお、安全の為、前記映像の提供に際しては、セキュリティ管理サーバSは適宜認証処理を行う。また、この参照に際し、図2の映像は、例えば、マウスなどのユーザインターフェースにより視点位置を移動させることが可能である。また、特定の種類のオブジェクトのみを表示させる機能（フィルタ機能）も備えており、例えば、何らかの処理を実行中である装置のみを表示させたり、外部ネットワークの装置からアクセスされている装置のみを表示させたりすることもできる。

## 【0076】

なお、図2の形態はあくまで一例に過ぎず、各オブジェクトの形状や色、模様、階層の分け方などの形態は、セキュリティ管理サーバSが提供する、例えば、図4に示すような設定用Webページを利用して、管理者やユーザなどが自由にカスタマイズすることができる。

## 【0077】

セキュリティ管理サーバSがLAN内の監視対象装置Cに提供する前記映像は、必ずしもリアルタイムなものに限られない。セキュリティ管理サーバSは、過去の映像も記憶管理しており、管理者やユーザは、過去のある時点やある期間における映像も適宜参照することができ、例えば、不正侵入等の異常があった場合における事後的な追跡調査にも威力を発揮する。

【0078】

#### ＜ログファイルの表示＞

ところで、一般に、ログ情報はその装置で行われた各種の処理がその内容と実行日時とを含むテキストメッセージで行別記載された構成のログファイルに管理されていることが多いが、このログファイルには、通常、膨大なテキストメッセージが含まれており、これをそのまま解析しようとするれば、非人間的な重労働を強いられることになる。また、ログファイルの解析には、それなりの技術が必要である。ここで説明するセキュリティ管理サーバの機能は、このような形式のログファイルの解析を容易に行えるように、ログファイルを人が利用しやすい形態に表示する機能である。

【0079】

図5はその一例である。最も左側のエリア21には、このログファイル中に含まれる所定のキーワードの出現頻度が示されている。キーワードは事業者AやLANの管理者等により適宜な内容に設定され、例えば、不正行為に用いられやすいコマンド（「su」コマンド）などが設定される。

【0080】

エリア22には、所定単位期間ごとのテキストメッセージの出力頻度が時系列的に横向き棒グラフで表示されている。棒グラフの長さは、短時間に多くのメッセージが出力される程長くなる。なお、時間区間は月単位、週単位、日単位等、様々なスケールに設定できる。

【0081】

エリア23には、各テキストメッセージの長さが横向き棒グラフで表示されている。各棒グラフはメッセージの種別に応じて色替えされている。

【0082】

エリア22,23に表示される棒グラフは、例えば、メッセージ長やメッセージ出力頻度の周期性もしくはその乱れを直感的に把握するのに好適であり、周期的もしくは不規則に行われる不正行為の発見には非常に有効な情報となる。

【0083】

なお、前記の映像におけるエリア21～23の表示内容は、例えば、ログファイルをテキストマイニング手法を適用するのに好適なフォーマットに変換し（変換処理）、変換後のログファイルについてテキストマイニング手法を適用し、前述のキーワードごとの時間別の出現頻度などの情報を抽出（抽出処理）し、これをグラフ化することで生成される。

【0084】

最も右側のエリア24には、ログファイルに記述されているテキストメッセージがそのまま表示されている。また、不正行為等の不正な事象を発見しやすくする為、指定されたキーワード（例えば「su」コマンド）が所定の色で強調表示され、出現頻度の高いキーワードが前記の色とは別の色で強調表示されている。

【0085】

<異常検知機能>

セキュリティ管理サーバSは、装置Cから収集したログ情報や、当該セキュリティ管理サーバS自身が記憶管理している自身のログ情報を対象として各種の分析アルゴリズムを実行し、例えば、外部ネットワークの不審な装置からLAN内の監視対象装置Cや自身に対してアクセス等があったかどうか、監視対象装置Cや自身への不審なログイン処理が繰り返された痕跡はないか、監視対象装置C上や当該セキュリティ管理サーバS上において不審なユーザによる特権ユーザへの切替えコマンドの実行、システムファイルなどの改竄・策のなどがされた痕跡はないか、といった各種のセキュリティ上の異常をリアルタイムに監視している。そして、セキュリティ管理サーバSは、この監視により異常を検知した場合にその旨やその内容を、例えば、前述した図2の映像に反映する。例えば、ある監視対象装置Cや自身にリモートログインしているユーザが「su」コマンドを入力するなどの不審な操作を行った場合には、そのユーザを示す球オブジェクト11が三角錐オブジェクト17に変化し、また、そのユーザが不審な操作を行った装置

とを結ぶ線分オブジェクト15が、点滅や色変化などにより強調表示される。

【0086】

また、セキュリティ管理サーバSは、当該サーバS内にあらかじめ登録されているLANの管理者やユーザのメールアドレスに、異常を検知した旨やその内容を記載した電子メールを行う機能も備えている。また、管理者やユーザなどは、電子メールの配信条件や配信時刻などをセキュリティ管理サーバSに登録しておくことができ、セキュリティ管理サーバSはその登録された条件に従って電子メールを送信する。

【0087】

＜ログ隠蔽処理に関連する情報の提供＞

ログ情報はセキュリティ管理上、重要な情報であるため、ログ情報そのものが不正行為のターゲットとなることも少なくない。そこで、事業者Aは、ログ情報自体に対する不正行為の防御手段として、セキュリティ管理サーバSが設置されているLAN内で稼働する監視対象装置Cに対し、つぎのような手段によるログ情報の隠蔽処理を行うソフトウェアの提供を行っている。

【0088】

このソフトウェアが提供する第一の機能は、ログ情報の実体であるログファイルを、その正本ファイルと、これとリアルタイムに同一内容に管理された複数の副本ファイルとの複数立てで管理し、これらを各監視対象装置C内に区画された複数の記憶場所（例えば、いわゆる「フォルダ」、「ディレクトリ」といった概念がこれに相当する）に分散して記憶する機能である。この機能によれば、例えば、あるログファイルに対して改竄や削除等の不正行為が行われたとしても、ログファイルの復旧を行うことが可能となる。

【0089】

また、前記ソフトウェアは、第二の機能として前記各副本ファイルを監視対象装置C内の他の記憶場所に適宜なタイミングで移送する機能を備えている。これにより不正侵入者等は副本ファイルの格納場所の特定が困難となりセキュリティの向上が図られることとなる。

【0090】

さらに、前記ソフトウェアは、第三の機能として、前記正副両ログファイルを適宜なタイミングでそれぞれ比較するなどしてこれらに対してセキュリティ上の異常がないかどうかを監視し、この監視により異常を検知した場合にその旨やその内容をセキュリティ管理サーバSに通知する機能を備えている。セキュリティ管理サーバSは、LAN内のある監視対象装置Cからこの通知があると、その旨やその内容を、例えば、所定のオブジェクトで表現するなどして、図2の映像などに反映させる。なお、セキュリティ管理サーバSは異常を検知した旨やその内容をホストサーバHに送信し、この情報は後述するホストサーバHにおけるLANの監視にも利用される。

## 【0091】

## ＜管理のための機能＞

セキュリティ管理サーバSは、LANの管理者やユーザの管理に便利のように、図6に示すようなLAN内の各監視対象装置Cに提供している各種サービスの内容を一覧表示したWebページを提供している。また、1つの組織に複数のセキュリティ管理サーバSを設置している場合などの便宜のため、このWebページの下半分には、組織内に設置されている各セキュリティ管理サーバSの稼働状況が一覧表示されている。

## 【0092】

## ＜DHCPに関する機能＞

セキュリティ管理サーバSが記憶管理するログ情報には、通常、それがどの監視対象装置Cについてのログ情報であるかの特定（識別）などに利用するその監視対象装置CのIPアドレスが付帯する。例えば、ある監視対象装置Cからこれと別の監視対象装置Cへのアクセスに関する事象が記述されたログ情報には、これら監視対象装置Cの一方もしくは双方のIPアドレスが付帯する。

## 【0093】

しかしながら、LAN内の各監視対象装置CへのIPアドレスの割り当てのために、LAN内にいわゆるDHCP（Dynamic Host Configuration Protocol）サーバが導入されている場合には、各監視対象装置Cに割り当てられるIPアドレスは動的に変化する可能性がある。このため、IPアドレスのみから監視対象

装置Cを特定する仕組みでは、例えば、同じ監視対象装置Cから収集したログ情報であるにもかかわらず、それぞれ別の監視対象装置Cのログ情報であると認識したり、異なる監視対象装置Cからのアクセスを同一監視対象装置Cからのアクセスであると誤認するといった問題を生じうる。

## 【0094】

そこで、この問題を解決するため、このセキュリティ管理サーバSは、DHCPサーバがIPアドレスの割り当てに際し記憶管理している、監視対象装置Cに割り当てたIPアドレスとその監視対象装置CのMACアドレスおよびその有効期間情報が逐次記録された対応表（以下、これを「割当履歴」と称する。一例を図7に示す。）を参照し、この割当履歴に基づき、記憶管理している前記各ログ情報がどの監視対象装置Cについてのものであるかを特定する仕組みを備えている。

## 【0095】

具体的には、例えば、セキュリティ管理サーバSは、各ログ情報について前記割当履歴から各ログ情報に付帯するIPアドレスに対応づけられているMACアドレスを検索し、その結果、同一のMACアドレスが対応づけられているログ情報には同一の装置名（ホスト名）を付帯させるなどして、同一のMACアドレスが対応づけられているログ情報は同一の監視対象装置Cからのものとして記憶管理する。

## 【0096】

なお、DHCPサーバの運用形態としては、セキュリティ管理サーバSとは独立したハードウェア上で動作する場合や、セキュリティ管理サーバS内にハードウェア的にもしくはソフトウェア的に組み込まれて動作する場合など、様々な形態が考えられる。このうち前者の場合、すなわち、DHCPサーバがセキュリティ管理サーバSとは独立したハードウェア上で動作する場合には、前記割当履歴をセキュリティ管理サーバSが取得するための仕組みが必要になるが、この仕組みは、例えば、DHCPサーバとセキュリティ管理サーバSとの間の適宜な通信により行われる。

## 【0097】

また、LAN内で複数台のDHCPサーバが稼働している場合には、同一のIPアドレスが異なる監視対象装置Cに割り当てられることがあるが、この場合は前記割当履歴に同じIPアドレスに異なるMACアドレスが対応づけされたものが混在することになり、これではIPアドレスからMACアドレスを一意に特定できない。そこでこのような場合には、セキュリティ管理サーバSは、前記割当履歴の各MACアドレスとIPアドレスの組み合わせに付帯して記録されている前記有効期間情報と、各ログ情報が生成された日時（この情報は、例えば、ログ情報自身に記録されている場合もあるし、セキュリティ管理サーバSがログ情報を収集した際に強制的に付帯させる場合などがある）とを比較して、この生成日時においてそのログ情報に付帯するIPアドレスが対応づけされていたMACアドレスを特定する。

## 【0098】

また、図8に示すように、負荷分散などを目的として、一つのLAN内に複数のセキュリティ管理サーバSを設置し、各セキュリティ管理サーバSのそれぞれにDHCPサーバを組み込むといった形態で運用されることがあるが、この場合、各セキュリティ管理サーバSは、それぞれが記憶管理している各DHCPサーバの前記割当履歴を、LANを通じて適宜に交換する。そして、各セキュリティ管理サーバSは、他のセキュリティ管理サーバSから送られてきた前記割当履歴と、自身が記憶管理している割当履歴とを統合管理し、これら割当履歴において同一のMACアドレスに対応づけられているIPアドレスが付帯するログ情報は全て同一の監視対象装置Cについてのものであるとして取り扱う。

## 【0099】

またさらに、これら複数のセキュリティ管理サーバSが、それぞれ独自にログ情報の視覚化などの前述した各種の機能を提供する場合には、各監視対象装置Cの装置名（ホスト名）は統一されていた方が実用上好ましい（例えば、図2に表示されている球オブジェクトに装置名（ホスト名）を付記する場合、その装置名は各セキュリティ管理サーバSで統一されていた方が好ましい）。そのため、セキュリティ管理サーバSは、MACアドレスと装置名（ホスト名）との対応づけを、他のセキュリティ管理サーバSとの間でLANを通じて適宜に交換する仕組

みも備えている。

【0100】

===ホストサーバの機能===

<セキュリティ管理サーバのメンテナンス>

図1に示すように、ホストサーバHは、各地のLANに設置されたセキュリティ管理サーバSと通信し、各セキュリティ管理サーバSの稼働状態をインターネットを通じて監視する。ホストサーバHには、各セキュリティ管理サーバSからインターネットを通じて稼働状況を通知するメッセージが送られてくる。

【0101】

ホストサーバHは、このメッセージの内容を監視する。そしてこの監視により何らかの異常を検知した場合には、その旨をモニタに表示する等して事業者Aに通知し、これにより異常を知った事業者Aは、この異常を通知してきたセキュリティ管理サーバSに対し、例えばインターネットや専用線などの通信手段を通じてリモートメンテナンスを行ったり、その設置現場にサービスマンを派遣するなどしてメンテナンスを行うこととなる。

【0102】

また、ホストサーバHは、各セキュリティ管理サーバSに対し、セキュリティ管理サーバS内で稼働する各種のソフトウェア（例えば、セキュリティ管理サーバ上で稼働するOSや、前述した映像の生成、各種機能を提供するソフトウェア）の機能追加、バグフィックス等のための更新データを、セキュリティ管理サーバSからのリクエストにより適宜に配信する。

【0103】

<ログ情報のバックアップ>

ホストサーバHは、セキュリティ管理サーバSから送られてくるログ情報を受信して、これをハードディスク等の記憶手段にバックアップ用として記憶管理する。

また、ホストサーバHは、当該装置が記憶管理している前記ログ情報を、セキュリティ管理サーバSに送信する。これにより、例えば、セキュリティ管理サーバSやLAN内で稼働する監視対象装置Cが管理しているログ情報が改竄や不正



削除などの被害にあった場合でも、ホストサーバHから送られてくるログ情報に基づいて改竄や不正削除等されたログ情報を復旧することができ、また、これを使って犯人の追跡調査などを行うことができる。

## 【0104】

## ＜設定情報の管理＞

セキュリティ管理サーバSは、ログ情報を視覚化する際にユーザが設定した、前述した各種映像の生成に際して適宜利用・参照される登録情報や、前記設定用Webページなどを利用して登録された前記ログ情報の収集対象となる監視対象装置Cについての登録情報などのセキュリティ管理サーバSが記憶管理している各種の設定登録情報を、適宜ホストサーバHに送信する。

## 【0105】

ホストサーバHは、セキュリティ管理サーバSから送られてくるこれらの設定登録情報を受信して、所定の記憶手段に記憶管理する。これらの情報は、セキュリティ管理サーバSの記憶エリアに十分な余裕があるかなどの運用上の各種状態確認や、セキュリティ管理サーバSがダウンした際におけるバックアップとして活用されるなど、セキュリティ管理サーバの各種メンテナンスに幅広く活用される。

## 【0106】

## ＜異常の検知＞

ホストサーバHは、セキュリティ管理サーバSから収集した前記ログ情報に基づいて、各セキュリティ管理サーバS、およびこれらが設置されているLAN内の各監視対象装置Cに不正侵入などのセキュリティ上の異常が無いかどうかを監視する。そして、ホストサーバHは、この監視により何らかの異常を検知すると、その旨やその内容をモニタに表示するなどして事業者Aに通知する。また、異常を検知した旨やその内容を、異常が検知されたLAN内に設置されたセキュリティ管理サーバSにインターネットを通じて通知する。セキュリティ管理サーバSは、前記通知を受信すると、その旨やその内容を例えば、図2の映像に反映させるなどして、そのLANの管理者やユーザなどに通知する。

## 【0107】

このようにホストサーバH側においてもログ情報の監視は行われ、これによりセキュリティ管理を確実に行うことができる。また、処理能力等の制限によりセキュリティ管理サーバSでは稼働させることができないような監視処理をホストサーバHで実行できる場合には、より強力にログ情報を監視することができる。

【0108】

＜携帯電話機に関する機能＞

ホストサーバHは、図9に示すようにインターネットを通じて携帯電話機Kと通信する機能を備える。ホストサーバHは、自身が行う前記の監視により異常を検知した場合に、インターネット接続機能を備えた携帯電話機Kに対し、インターネットを通じてその旨やその内容を通知するサービスも提供する。このサービスは、例えば、携帯電話機Kの電話番号やメールアドレスの登録を済ませた者に提供される。これにより、例えば、LANの管理者やユーザは、外出先などにおいても、LAN内の監視対象装置Cに異常があったことを知ることができる。

【0109】

また、ホストサーバHは、携帯電話機から送られてくるログ情報の問い合わせメッセージを受信して、応じてログ情報を検索し、その結果を所定の映像に編集して前記携帯電話機に送信する機能も備えている。LANの管理者等は、この機能を利用して、例えば、外出先などからでも監視対象装置Cのログ情報の調査や分析を行うことができ、これにより迅速な対応が可能となる。

【0110】

また、ホストサーバHは、インターネットを通じて所定の携帯電話機Kから送られてくるLAN内で稼働する監視対象装置Cを特定する情報とその監視対象装置Cで実行される処理コマンドとを受信して、その処理コマンドをインターネットを通じて監視対象装置Cに送信する。そして、ホストサーバHは、前記監視対象装置Cにおいて前記処理コマンドが実行され、その実行結果が前記監視対象装置Cから送られてくると、これを前記携帯電話機Kのユーザインターフェースに適した形態の映像に編成して前記携帯電話機Kに送信する。この処理は、例えば、ホストサーバHと前記監視対象装置Cとの間の遠隔制御機能（例えば、UNIXにおける「telnet」）などの機能を利用して行われる。

## 【0111】

また、前記処理コマンドは、例えば、この処理コマンドが実行される監視対象装置CのOSがUNIXである場合には、LAN内の各監視対象装置Cの接続状況を監視する「netstat」コマンド、ユーザのログイン・ログアウトの時間や接続元コンピュータを表示する「last」コマンド、ログイン中のユーザやコマンドの監視する「w」コマンド、ファイルシステムのディスク容量の使用状況を表示させる「df」コマンド、システム状況とCPUの使用状況を表示させる「top」コマンド、ログの状況を調査する「syslog」コマンドなどである。

## 【0112】

この機能によれば、LANの管理者等は、日頃から使い慣れた処理コマンドにより携帯電話機Kを利用して、所定の監視対象装置Cに格納されているログ情報を閲覧することができる。

## 【0113】

## &lt;通信パケットを利用した実施例&gt;

ところで、以上に説明した仕組みはログ情報を利用するものであったが、セキュリティ管理サーバSは、LAN上を流れる通信パケットを利用してセキュリティ管理に有用な各種の映像を提供する機能も備えている。この仕組みの概念図を図10に示す。

## 【0114】

一方、図11はこの仕組みにおいてセキュリティ管理サーバSが通信パケットを取得する仕組みを示している。取得対象の通信パケットは、例えば表1に示すようなものであるが、パケットの種類は必ずしもこれらに限定される訳では無い。

## 【0115】

【表 1】

プロトコル	監視プロトコル(ポート)	監視コマンド
T C P	WindowsNT / 2000ドメイン	login
	telnet	login / logout
	ftp	login / close / quit
		cd / lcd
		get / put / delete / rmdir(マルチも含む)
	pop3 / imap4 / apop	コマンド(USER ~ QUIT)
		From / To / cc / bcc
	smtp	From / To / cc / bcc
	http	URL /
	rpc / rlogin / rsh / rcp / rexec	login / コマンド
	NetBIOS over TCP/IP (ファイル共有/ネットワーク印刷)	SMB
NetBEUI	(ファイル共有/ネットワーク印刷)	

## 【 0 1 1 6 】

セキュリティ管理サーバSはつぎのような方法によりLAN上を流れる通信パケットを収集する。例えば、セキュリティ管理サーバSは自身と同一のHubに接続する監視対象装置Cにて送受信される通信パケットについては、当該サーバS自身が直接取得可能であるので当該サーバSが直接取得する（但し、セキュリティ管理サーバSが接続しているHubがスイッチングHubのようなインテリジェント機能を持つ場合を除く）。他方、サーバS自身がスイッチングHubに接続している場合や、サーバSが接続しているHubと異なるHubに接続する監視対象装置Cにて送受信される通信パケットについてはサーバS自身が直接取得することはできないが、これらの通信パケットについては、例えば、監視対象装置C側で通信パケットを取得するプログラム（通信監視ソフトウェア）を稼働させ、このプログラムの作用により監視対象装置C内に蓄積記憶されている通信パケットを適宜なタイミングでLANを通じてセキュリティ管理サーバSに集信

するようにすることで取得する。

【0117】

なお、セキュリティ管理サーバSが監視対象装置C内の通信パケットを取得する具体的な仕組みとしては、例えば、監視対象装置Cにて通信パケットが格納されているファイルをLAN上で参照可能に共有化しておき、これをセキュリティ管理サーバSから参照しLANを通じて複写するといった方法がある。また、例えば、監視対象装置Cに蓄積記憶されている通信パケットが格納されているファイルを、データもしくはファイルとして適宜なタイミングでLANを通じてセキュリティ管理サーバSに送信させるといった方法もある。なお、これらいずれの方法においても、各監視対象装置Cから通信パケットが記録されたファイルを集めるタイミングは、タイマーによる日時指定、装置Cに記憶管理されている通信パケットの数やデータサイズがある一定量に達したところで収集するなど、ユーザのニーズや視覚化する映像の内容などに応じて適宜に設定されることになる。

【0118】

セキュリティ管理サーバSは、以上のようにして収集した通信パケットを、図12に示すデータフォーマットからなるパケット情報ファイルとして記憶管理する。一方、セキュリティ管理サーバSは、適宜パケット情報ファイルから視覚化処理に好適な情報を抽出してこれらを各監視対象装置C別に整理した図13に示すデータフォーマットからなる視覚化基礎データ（パケットログファイル）を生成し、これをデータベースに記憶管理する。ここでこの監視対象装置C別の整理に際しては、パケット情報ファイルに含まれている通信パケットのそれぞれがどの監視対象装置Cに関するものであるかを特定する必要があるが、この特定は、例えば、各通信パケットの送信先もしくは受信先のIPアドレスを利用して行う。なお、前述の「DHCPに関する機能」のところで説明したように、IPアドレスのみからでは監視対象装置Cを一意に特定できない場合もあるが、この場合には前述と同様に通信パケットに記述されているMACアドレスも利用して監視対象装置Cの特定を行う。

【0119】

セキュリティ管理サーバSは、このようにして生成されデータベースに記憶管理されている視覚化基礎データに基づいて、LAN内のセキュリティ管理に有用な各種の映像を生成する。以下、これらの映像の具体例を紹介する。なお、セキュリティ管理サーバSにより生成されるこれらの映像は、Webページへの組み込み映像としてLAN上で稼働する監視装置Cに適宜提供され、これらの映像は、LANに接続する各監視装置Cのユーザが自由に（但し、各LANの運用ポリシーに応じて適宜アクセス制限が施されることはある）参照することができる。つまり、不正な事象の発見などのLAN内のセキュリティ管理を各ユーザが共同して行うことができる。

#### 【0120】

視覚化基礎データに基づく映像の一例を図14に示す。この映像にはある会社のオフィス内に敷設されたLANの状態が示されている。各フロアに相当する部分には、各フロアに設置されているパソコンの台数がコンピュータ形状の図案の数により示されている（この例では、稼働中のパソコン10台に対して1台のパソコンが描画されている）。また、各階のLANを流れる通信パケットの数を示す棒グラフも表示されている。ちなみに、これら台数や通信パケット数などの統計情報は、視覚化基礎データに記述されているパケット収集時間などを利用して求められる。なお、この図の生成には、オフィスビルの構成情報、例えば、ビルが何階建てであるかであるといった各フロアの部署名などの情報も必要であるが、これらの情報はセキュリティ管理サーバSの管理者や監視対象装置Cのユーザなどが、あらかじめWebページなどを利用してセキュリティ管理サーバSに登録しておく。

#### 【0121】

一方、セキュリティ管理サーバSは、例えば、LAN内のある監視対象装置Cに対してアクセスが許可されていない監視対象装置Cからアクセスされていたり、監視対象装置C上で動作するプログラム（もしくは、TCP/UDPの通信ポート番号）やデータベースについてその利用を許可されていないユーザからのアクセスが行われているようなことがないか（これらを以下「権限外アクセス」と称する）といったことをリアルタイムに監視している。そして、権限外アクセス

があったことを検知すると、例えば、権限外アクセスが行われている監視対象装置Cが設置されたフロアの部分に所定の形態の模様を点滅表示させる。

## 【 0 1 2 2 】

ここで前記の監視は、図 1 5 に示すように、例えば、セキュリティ管理サーバSにあらかじめ各監視対象装置Cについて、各監視対象装置Cへのアクセスを許可する監視対象装置CのIPアドレスをアクセス制限情報として記憶管理しておき、ある監視対象装置Cについての視覚化基礎データ中にその監視対象装置Cについてのアクセスが許可されていないIPアドレスを有する監視対象装置Cからのアクセスの履歴が存在するかどうかを調べる、といった方法で行われる。また、監視対象装置C上で動作するプログラムやデータベースについて、その利用を許可されていないユーザからのアクセスが行われているかについての調査は、例えば、セキュリティ管理サーバSにあらかじめ各監視対象装置C上で稼働するプログラムやデータベースごとにそのプログラムやデータベースを利用可能なユーザIDをアクセス許可情報として記憶管理しておき、ある監視対象装置Cについての視覚化基礎データ中にその監視対象装置C上で稼働するプログラムがその利用が許可されていないユーザIDにより利用された痕跡が無いかどうかを調べることにより行う。

## 【 0 1 2 3 】

視覚化基礎データに基づく映像の他の一例を図 1 6 に示す。この図は、図 1 4 におけるあるフロア内のLANの利用状況をより詳細に示すもので、この映像には通信パケットに基づいて生成されるLAN内の各監視対象装置C間で行われる通信の状態や各監視対象装置Cへのユーザの利用状況、各監視対象装置Cで動作するデータベースへの各監視対象装置Cもしくはユーザからのアクセス状況などの情報を視覚化した映像が、前記LAN内で稼働する各監視対象装置Cの抽象図案を各監視対象装置Cの現実の配置状態に則した形態に配置した映像に重ねて描画されている。なお、この図は例えば、図 1 4 におけるフロア部分がマウスでクリックされた場合などに適宜表示される。図 1 6 の映像に必要な座席のレイアウトや各座席部分に表示されるその座席の利用者の氏名などの情報は、セキュリティ管理サーバSの管理者やLAN上の各監視対象装置Cを利用するユーザなどが

あらかじめセキュリティ管理サーバSに登録しておく。

【 0 1 2 4 】

図 1 6 の映像の各座席の部分には、その座席に設置されている監視対象装置Cが現在どのような種類（プロトコル）で通信を行っているか、どのようなシステムやプログラム、データベースを利用しているかといった情報を、色分けや図案（利用中のプロトコルに対応する形状のアイコンなど）などにより視覚的に表現した映像が描画される。また、アクセスする側とされる側の監視対象装置C同士が同色に表示されるなどして通信の状態を把握しやすいように工夫してある。また、図 1 4 の映像の場合と同様に図 1 6 の映像においても権限外アクセスの事象が示され、例えば、ある監視対象装置Cについて権限外アクセスが行われている場合には、その監視対象装置Cが設置されている座席の部分が点滅表示される。

【 0 1 2 5 】

図 1 7 は視覚化基礎データに基づく映像の他の一例である。この映像は図 1 6 の映像の一部をクローズアップしたもので、監視対象装置Cを利用中のユーザのユーザ名や顔写真など、図 1 6 よりも詳細な情報が含まれている。また、この図にも図 1 6 と同様に権限外アクセスの状況が示される。なお、この図は例えば図 1 6 の所定の部分がマウスでクリックされた場合などに表示される。

【 0 1 2 6 】

図 1 8 の映像は図 1 7 のある座席の部分をマウスでクリックするなどされることで表示され、クリックされた座席に設置されている監視対象装置Cについての情報（例えば、その監視対象装置Cに割り当てられているIPアドレス）やその監視対象装置Cのユーザに関する情報（例えば、そのユーザの電子メールアドレス、監視対象装置Cを利用してその監視対象装置Cのユーザにより行われた各種システムや各種サーバへのログイン履歴、プリンタなどの各種共用ネットワーク資源の利用履歴、監視対象装置C上で稼働するソフトウェアの当該装置Cのユーザによる利用履歴や各種ファイルの更新履歴など）が表示される。なお、この映像の提供に際しては、各ユーザのセキュリティ確保のため、適宜認証処理が行われる。

【 0 1 2 7 】



図 1 9 ～ 2 1 は視覚化基礎データに基づく映像の他の一例である。図 1 9 の映像には、業務システムや社内管理システム、グループウェアなどの各システムの運用を行っている前記 LAN 内の監視対象装置 C の稼働状態、およびこれら各監視対象装置 C に対する他の監視対象装置 C からの単位時間あたりのアクセス頻度が、各監視対象装置 C を利用して運用されるシステム別に分類されて表示されている。

#### 【 0 1 2 8 】

図 2 0 の映像には、業務システムや社内管理システム、グループウェアなどの各システムの運用を行っている監視対象装置 C への単位時間あたりのアクセス頻度が棒グラフにより表示されている。なお、アクセス頻度は各システムで稼働する各サーバコンピュータへのアクセス頻度をシステム単位で集計したものであり、例えば、視覚化基礎データに基づいて各サーバに出入りする単位時間ごとの通信パケット数を集計して計算したものである。

#### 【 0 1 2 9 】

図 2 1 の映像には、各システムで稼働する監視対象装置 C ごとのアクセス頻度が棒グラフで表示されている。また、この図には各監視対象装置 C 内で稼働するデータベースごとのアクセス頻度も表示される。ここでこのアクセス頻度は、例えば、SQL 文を含んだ通信パケットに基づく視覚化基礎データを抽出し（図 2 2）、その視覚化基礎データ中に記載されているデータベース名などのデータベースを特定し、特定されたデータベースごとに出現頻度を累計するといった方法で算出される。なお、図 1 9 ～ 2 1 の映像は、単独で表示することもできるし、図 1 4 や図 1 6、図 1 7 の映像と組み合わせて表示することもできる。また、権限外アクセスがあれば、図 1 9 ～ 2 1 の各映像にはその事象が点滅表示などの所定の形態で示される。

#### 【 0 1 3 0 】

#### < プログラム実行履歴の視覚化 >

ところで、セキュリティ管理サーバ S は、監視対象装置 C におけるプログラムの実行履歴に基づいて LAN 内におけるセキュリティ管理に有用な映像を生成し、これを監視装置 C に送信する機能も備えている。図 1 0 に示すように、監視対

象装置Cにおける実行履歴は、監視対象装置C上で常駐動作するプログラム実行監視ソフトウェアによって行われる。プログラム実行監視ソフトウェアは、監視対象装置C上でプログラムが実行されたことを検知して、そのプログラムの実行開始時刻や終了時刻、メールの送受信情報、ブラウザの操作情報、プリンタの使用状況、そのプログラムにより参照されたファイル名などの情報を実行履歴として蓄積記憶する。なお、プログラム実行監視ソフトウェアはこれらの情報を、例えば、プログラム起動時やファイル参照時に監視対象装置C上で動作するOSが発する各種メッセージ情報を監視することで取得する。

## 【0131】

セキュリティ管理サーバSは、適宜監視対象装置Cから前記実行履歴をLANを通じて収集してこれらを監視対象装置C別に記憶管理し、これら実行履歴を適宜LAN内のセキュリティ管理に有用な形態の視覚化した映像を生成する。そして、この映像はLANを通じて適宜セキュリティ管理サーバSから監視装置Cに送信され、監視装置Cのディスプレイ等に表示されることになる。

## 【0132】

===その他===

また、前述したように、ログ情報はセキュリティ管理上、非常に重要かつ有用な情報であり、改竄や不正削除等の対象になりやすい。従って、その管理はなるべく慎重に行う必要がある。以上の実施例では、セキュリティ管理サーバSとLAN内の各監視対象装置Cとの間、セキュリティ管理サーバSとホストサーバHとの間、携帯電話機KとホストサーバHとの間などにおけるログ情報を送受信するに際し、認証処理や暗号化等の処理を行うかどうかについて言及していないが、これらの通信に際しては、適宜、認証処理や暗号化等が施されることになる。

## 【0133】

## 【発明の効果】

以上に説明したように、会社内など組織内のLAN内に設置されて機能する本発明のセキュリティ管理サーバは、当該LAN内で稼働する各監視対象装置のログ情報やLAN内を流れる通信パケットを自動的に収集し、収集したログ情報や通信パケットからLANのセキュリティ管理に有用な情報を抽出してこれを人が

利用しやすい形態に視覚化した映像を生成し、前記映像を前記 LAN を通じて監視装置に送信するといった各種の機能を提供する。

【 0 1 3 4 】

従って、各監視対象装置に格納されているログ情報や通信パケットが自動的に収集され、ログ情報等の収集を効率よく行うことができる。また、収集したログ情報等からセキュリティ管理に有用な情報が自動的に抽出され、その情報は人が利用しやすい形態に視覚化された映像として提供されるので、従来に比べてログ情報の調査・分析等の作業が格段に省力化されることになる。また、このように視覚化されることで、単にログファイルや通信パケットを眺めていただけでは気づけなかったようなセキュリティ管理に有用な事象も発見しやすくなり、より確実なセキュリティ管理を行うことができるようになる。

【 0 1 3 5 】

また、前記の映像は前記 LAN を通じて監視装置、例えば、管理者のコンピュータや日常のデスクワークに使用されている個人用パソコンなどに提供され、これにより LAN 内で稼働する各種監視対象装置の利用者が共同して LAN 内のセキュリティ管理を行うことができるようになり、熟練者や専門のオペレータがいなくても充実したセキュリティ管理を行うことができる。また、各利用者が互いに LAN 内のセキュリティを監視することで、いわゆる内部者による不正行為等の防止策としても有効に機能する。

【 0 1 3 6 】

また、従来から研究されている不正侵入の検知や発見、対策などについての豊富な経験に基づき、収集したログ情報を不正侵入等の不正行為に適した状態に視覚化してユーザにログ情報を提示するようにしていたため、ログファイルの中身を一行ずつ追っていくような非人間的な作業を強いられることなく、容易に不正行為を発見することができる。

【 0 1 3 7 】

また、携帯電話機からもログ情報を参照できるようにしたため、例えば、休日や出張時などに出先から LAN 内で稼働する監視対象装置の遠隔監視等を行うことも可能である。さらに、携帯電話機に、LAN 内の装置に異常があったことが

自動的に通知されるため、管理者やユーザ等は、LAN内で起きた不正行為等の異常をより迅速に知ることができ、被害の拡大を最小限に抑えることができる。

【図面の簡単な説明】

【図 1】

本発明の一実施例によるセキュリティ管理サーバが設置されたLANの概略的なネットワーク構成を示す図である。

【図 2】

本発明の一実施例によるセキュリティ管理サーバが生成する映像の一例を示す図である。

【図 3】

図 2 の映像の部分拡大図を示す図である。

【図 4】

本発明の一実施例による図 2 の映像の設定用Webページを示す図である。

【図 5】

本発明の一実施例によるログファイルを視覚化した映像を示す図である。

【図 6】

本発明の一実施例によるLAN内の各装置に提供している各種サービスの内容を一覧表示したWebページを示す図である。

【図 7】

本発明の一実施例による、DHCPサーバにおいて記憶管理される割当履歴の一例、およびMACアドレスと装置名（ホスト名）の対応表の一例を示す図である。

【図 8】

本発明の一実施例による、セキュリティ管理サーバがLAN内に複数台設置された場合における、各セキュリティ管理サーバ間での割当履歴が交換される様子を示す概念図である。

【図 9】

本発明の一実施例によるLAN、セキュリティ管理サーバ、ホストサーバ、および携帯電話機などの関連を示す、概略的なネットワーク構成を示す図である。

【図 1 0】

本発明の一実施例による、セキュリティ管理サーバによる、通信パケットを利用してセキュリティ管理に有用な各種の映像を提供する仕組みを説明する図である。

【図 1 1】

本発明の一実施例による、セキュリティ管理サーバが通信パケットを取得する仕組みを説明する図である。

【図 1 2】

本発明の一実施例による、パケット情報ファイルのデータフォーマットを示す図である。

【図 1 3】

本発明の一実施例による、視覚化基礎データのデータフォーマットを示す図である。

【図 1 4】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 1 5】

本発明の一実施例による、セキュリティ管理サーバが権限外アクセスを監視する仕組みを説明する図である。

【図 1 6】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 1 7】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 1 8】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 1 9】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 2 0】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 2 1】

本発明の一実施例による、視覚化基礎データに基づく映像の一例を示す図である。

【図 2 2】

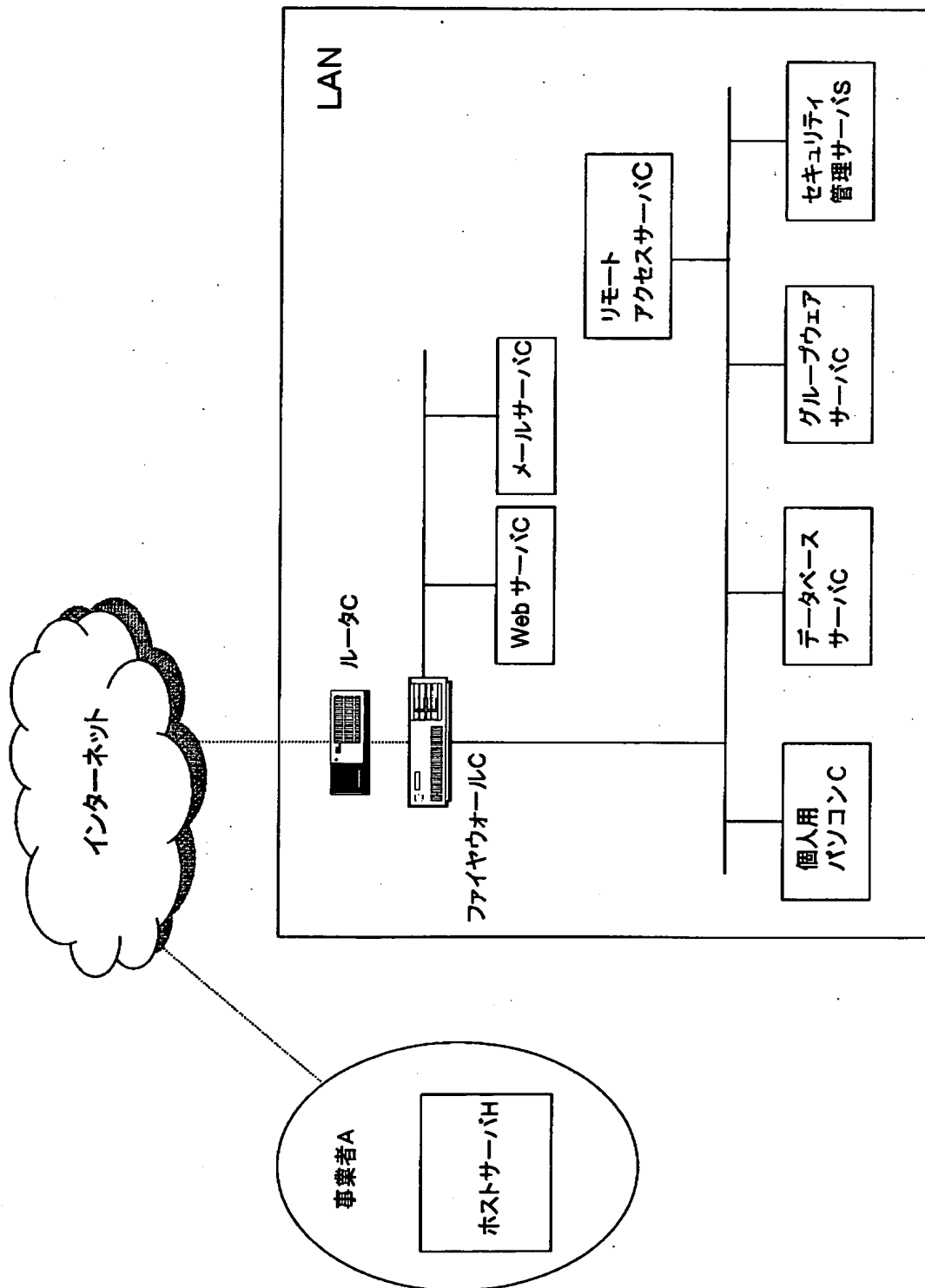
本発明の一実施例による、データベースを特定する仕組みを説明する図である。

【符号の説明】

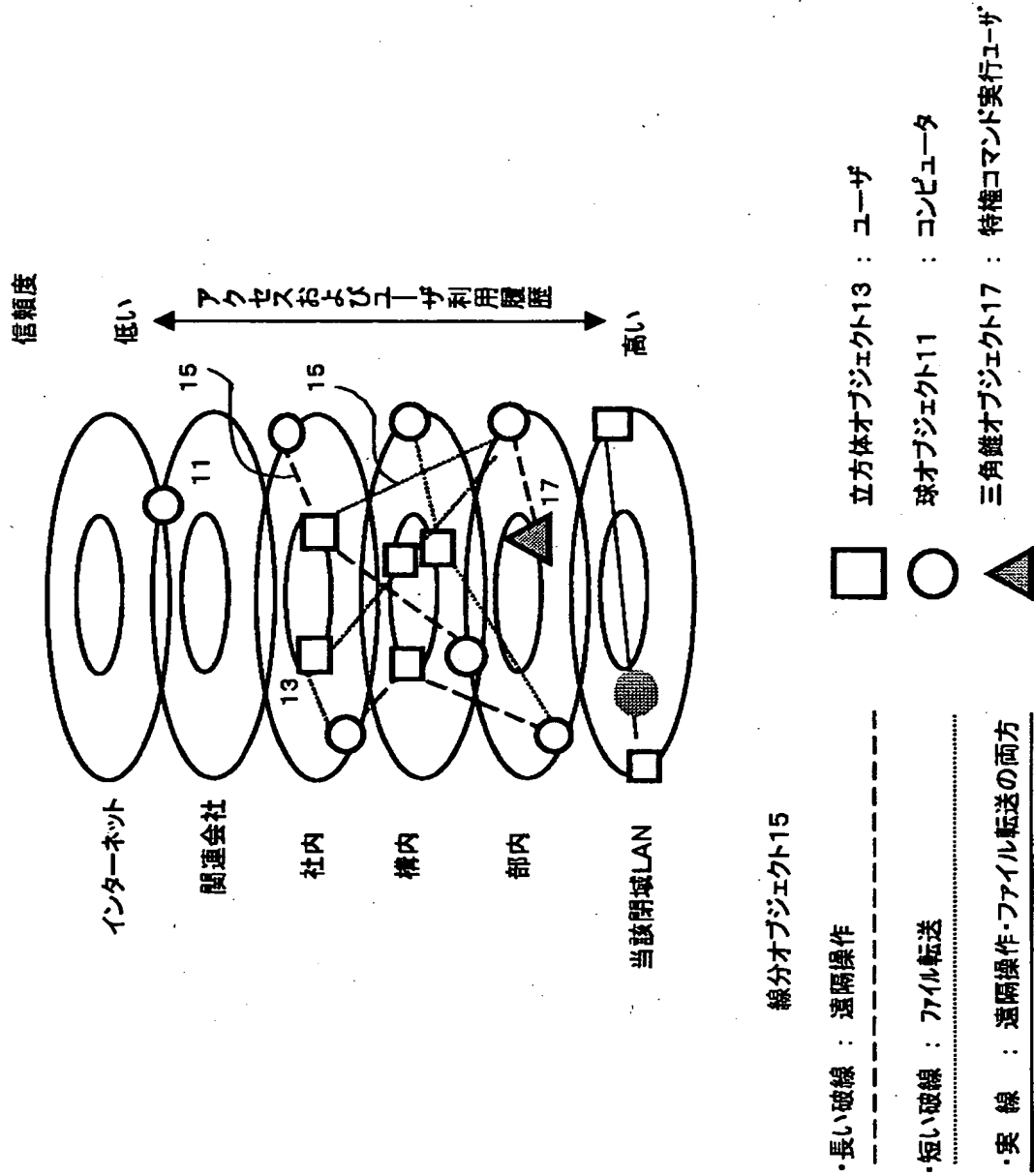
- S セキュリティ管理サーバ
- C 監視対象装置または監視装置
- H ホストサーバ
- K 携帯電話機

【書類名】 図面

【図 1】

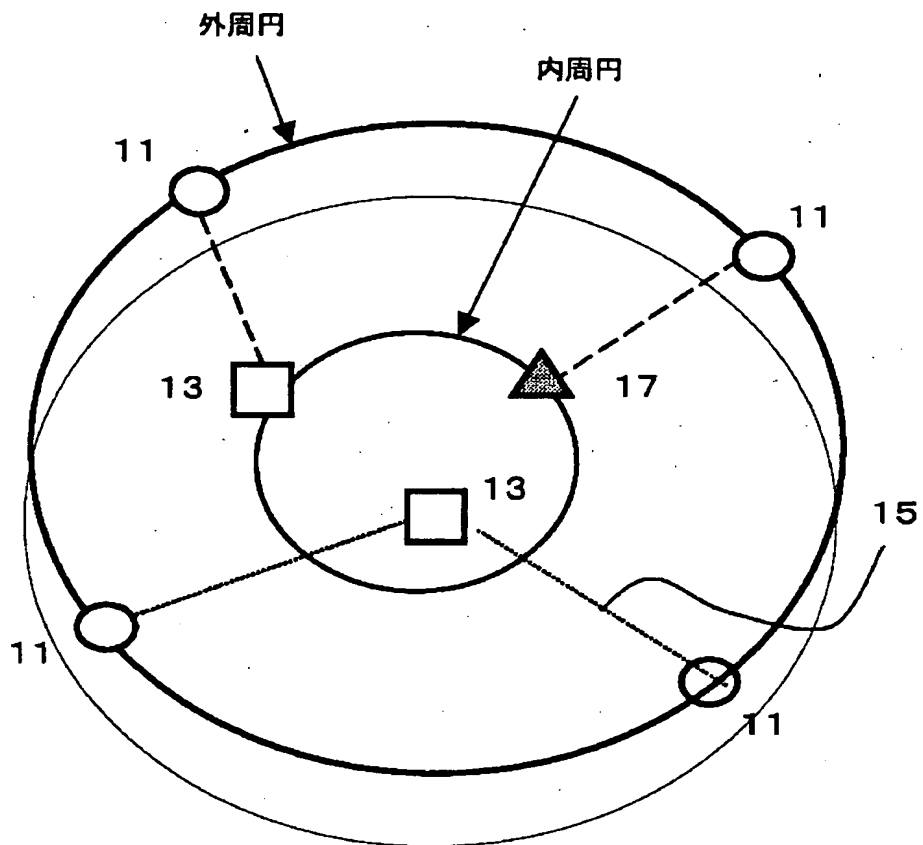


【図2】





【図 3】



【図4】

対象装置		レイヤーの表示方法(グループ分類)					表示時間			表示角度操作	
		ドメイン別	部門別	ビル階層別	アクセス種別	リアルタイム	フルタイム	フルバック	デフォルト	任意	
1	個人用パソコン			○		○				○	
2	データベースサーバ				○	○				○	
3	Webサーバ	○				○			○		
4	メールサーバ		○					○	○		
5											
6											
7											
8											
9											
10											
環境設定		OS					DHCP環境			ログ収集時間	
		unix	unix	unix	Windows	OPEN	SEER	DHCP	5分	任意	
1	個人用パソコン	○						○	○		
2	データベースサーバ	○						○	○		
3	Webサーバ			○		○			○		
4	メールサーバ			○		○				240分	
5											
6											
7											
8											
9											
10											

【図 5】

```

Jun 25 01:01:05 comp1 syslogd: restart
Jun 25 02:25:56 comp1 fipd[28856]: connection from kawa.yama.uec.ac.jp
Jun 25 02:25:56 comp1 fipd[28856]: FTP LOGIN FROM kawa.yama.uec.ac.jp as mana
Jun 25 03:00:05 comp1 hft[28297]: no rw file systems in mtab
Jun 25 03:00:05 comp1 fcr[29374]: fcr_xls -m /etc/mtab -t 7200 -f /var/tmp/.
Jun 25 03:30:38 comp1 Xaession: mana: login
Jun 25 05:18:03 comp1 fipd[28785]: connection from kawa.yama.uec.ac.jp
Jun 25 05:18:03 comp1 fipd[28785]: FTP LOGIN FROM kawa.yama.uec.ac.jp as mana
Jun 25 05:27:52 comp1 Xaession: mana: logout
Jun 25 06:37:52 comp1 Xaession: mana: login
Jun 25 12:48:15 comp1 login[31071]: ?@mura.yama.uec.ac.jp as cynthia
Jun 25 21:13:25 comp1
Jun 25 21:14:16 comp1
Jun 25 21:30:43 comp1 nix: WARNING: ARP: got MAC address
Jun 25 21:30:43 comp1 Xaession: mana: logout
Jun 25 03:42:18 comp1 fipd[31806]: connection from kawa.yama.uec.ac.jp
Jun 26 03:42:18 comp1 fipd[31806]: FTP LOGIN FROM kawa.yama.uec.ac.jp as mana

Jun 25 01:01:05 comp1
Jun 25 02:25:56 comp1
Jun 25 02:25:56 comp1
Jun 25 03:00:05 comp1
Jun 25 03:30:38 comp1 Xaession: mana: login
Jun 25 05:18:03 comp1 fipd[28785]: connection from kawa.yama.uec.ac.jp
Jun 25 05:18:03 comp1 fipd[28785]: FTP LOGIN FROM kawa.yama.uec.ac.jp as mana
Jun 25 05:27:52 comp1 Xaession: mana: logout
Jun 25 06:37:52 comp1 Xaession: mana: login
Jun 25 12:48:15 comp1 login[31071]: ?@mura.yama.uec.ac.jp as cynthia
Jun 25 21:13:25 comp1 Xaession: mana: login
Jun 25 21:14:16 comp1 unix: WARNING: ARP: got MAC address
Jun 25 21:30:43 comp1 Xaession: mana: logout
Jun 26 03:42:18 comp1 fipd[31806]: connection from kawa.yama.uec.ac.jp
Jun 26 03:42:18 comp1 fipd[31806]: FTP LOGIN FROM kawa.yama.uec.ac.jp as mana

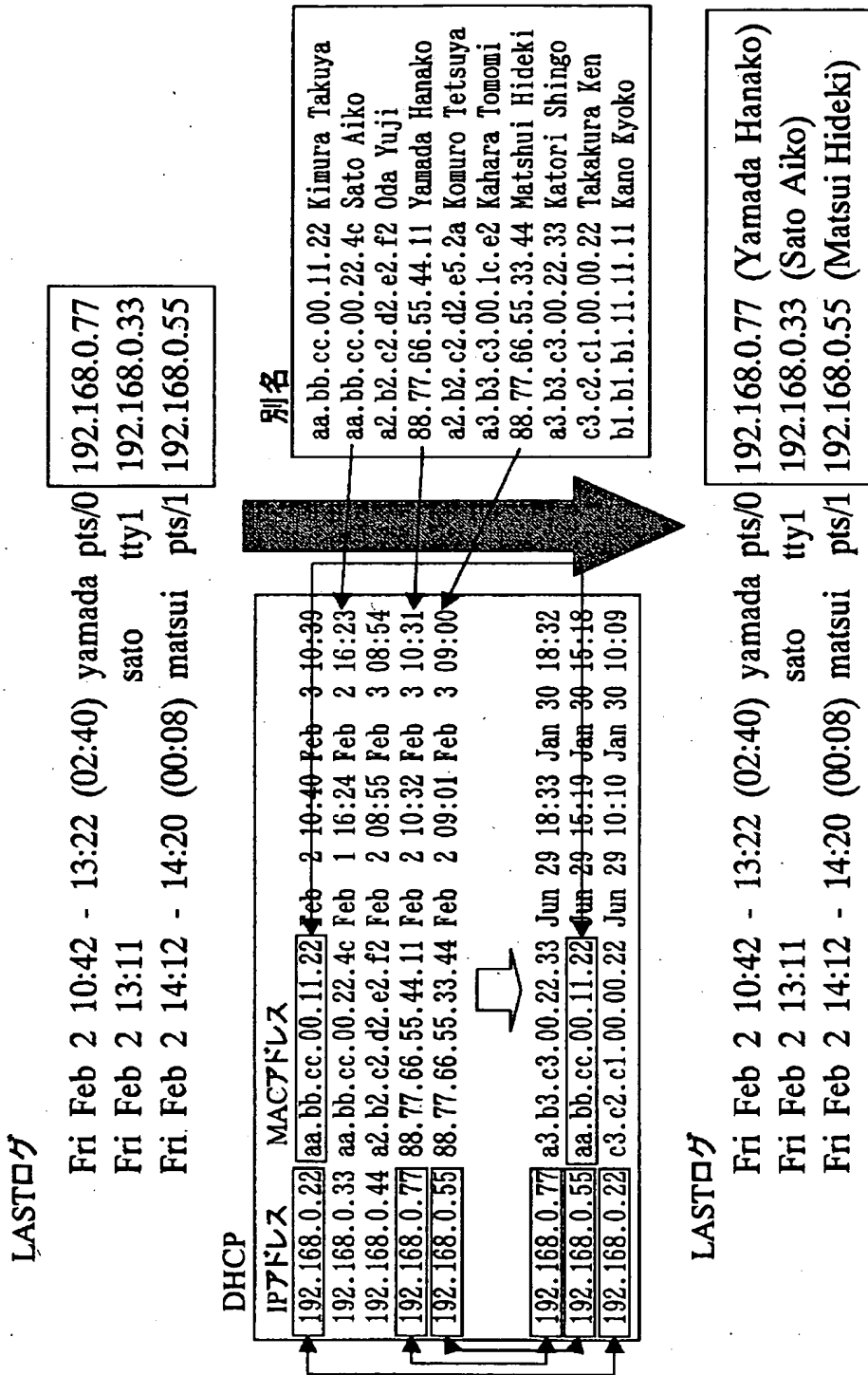
```

21	22	23	24
----	----	----	----

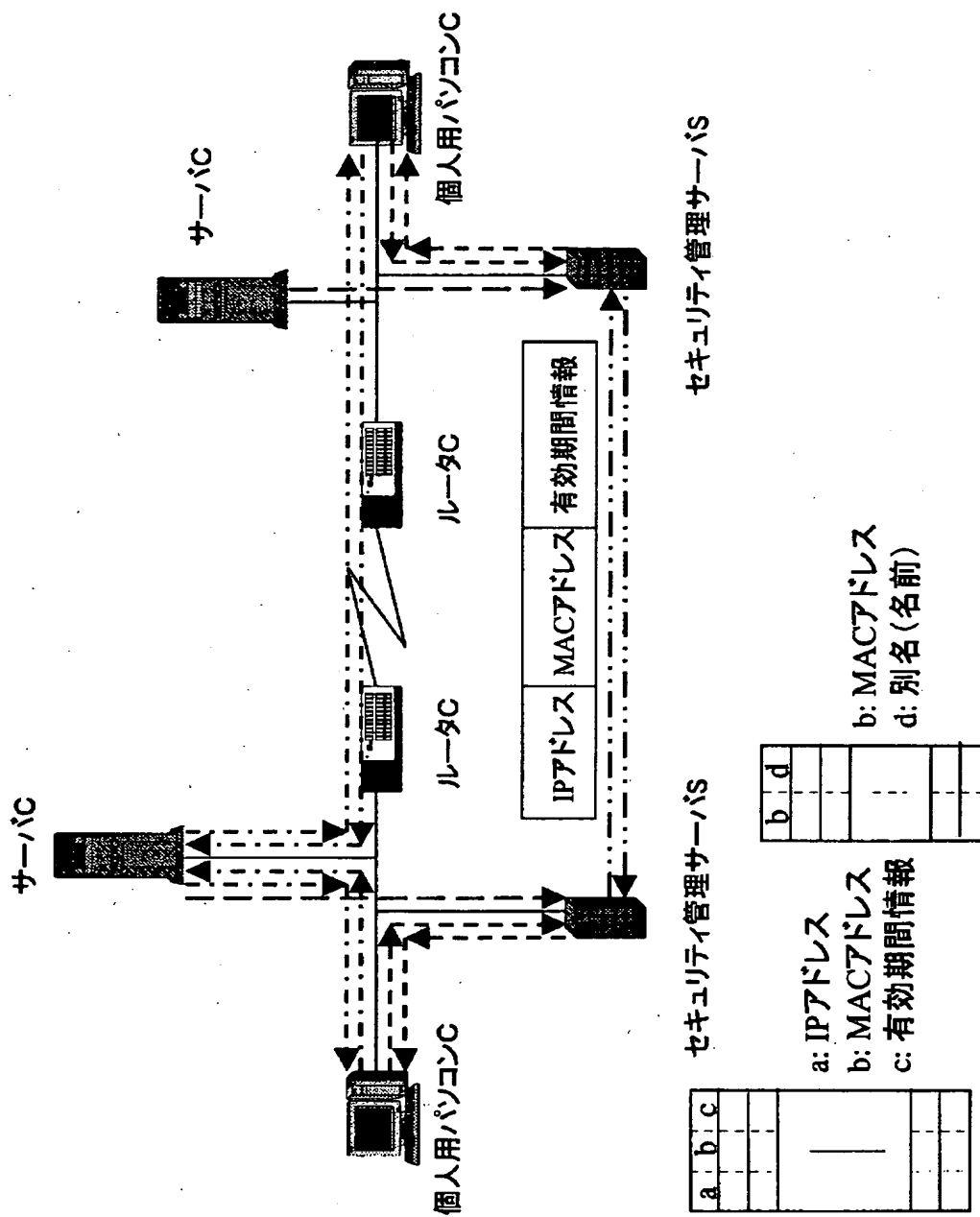
【図6】

〇〇〇 株式会社		CSO：向井 徹		システム管理者：足立 正浩		
管理対象コンピュータ		スペック	サービス内容			
			基本機能	3D視覚化	リモート監視	ログ隠蔽
1	DBSサーバ1	Solar	○	○	○	○
2	DBSサーバ2	Solar	○	○	○	○
3	Webサーバ	Linux/ 1C	○	○	○	○
4	Mail	Linux/ 1C	○	○	○	○
5	RAS Gateway	Solar	-	○	-	○
6						
7						
● 管理サーバの稼働状況						
稼働状況		設置場所	管理対象コンピュータ			
			1	2	3	4
1	正常	社長室	DBSサーバ1	DBSサーバ2	Webサーバ	メールサーバ
2	正常	情報管理室	リモートGateway			
3						
4						
5						

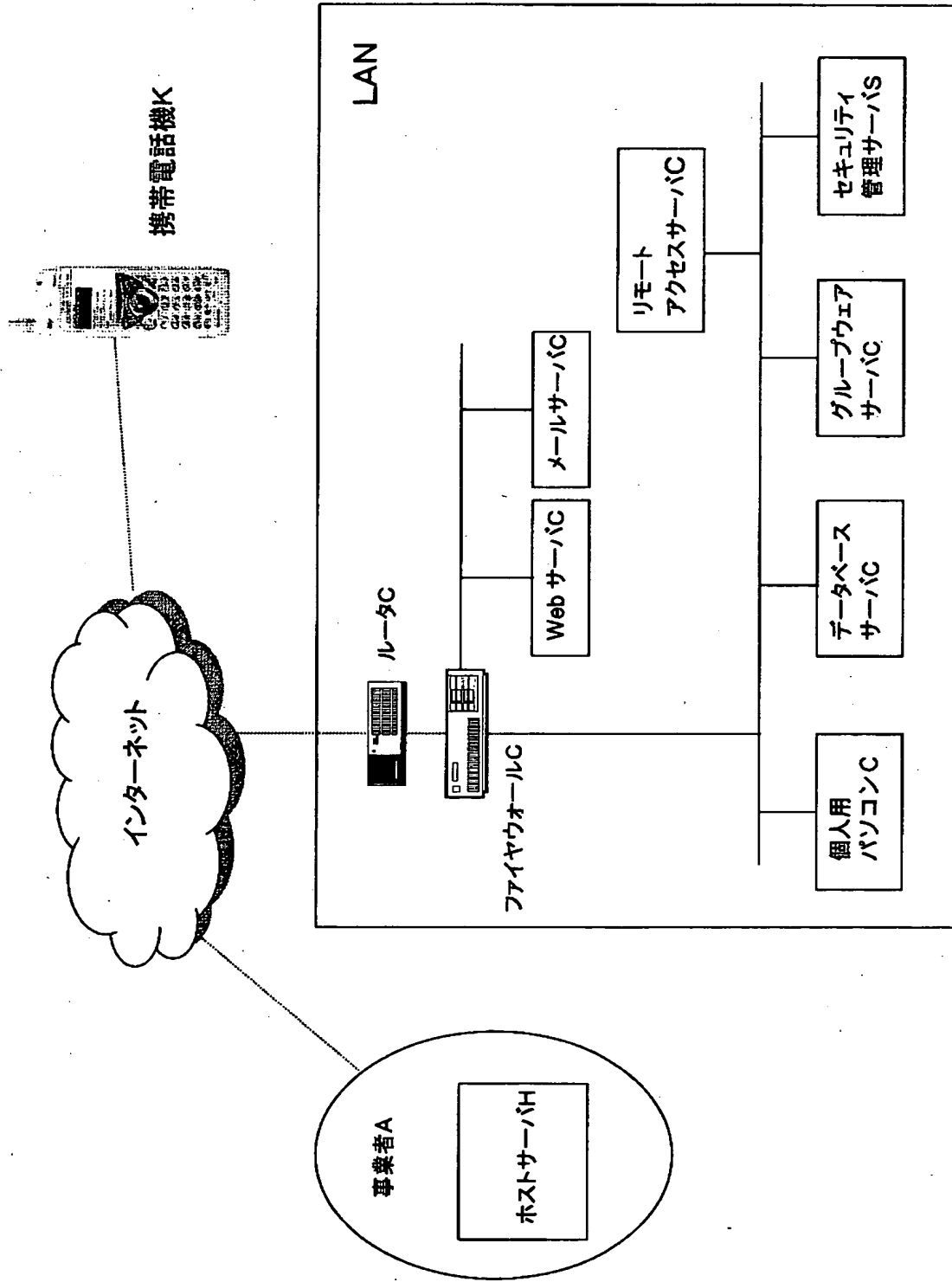
【図 7】



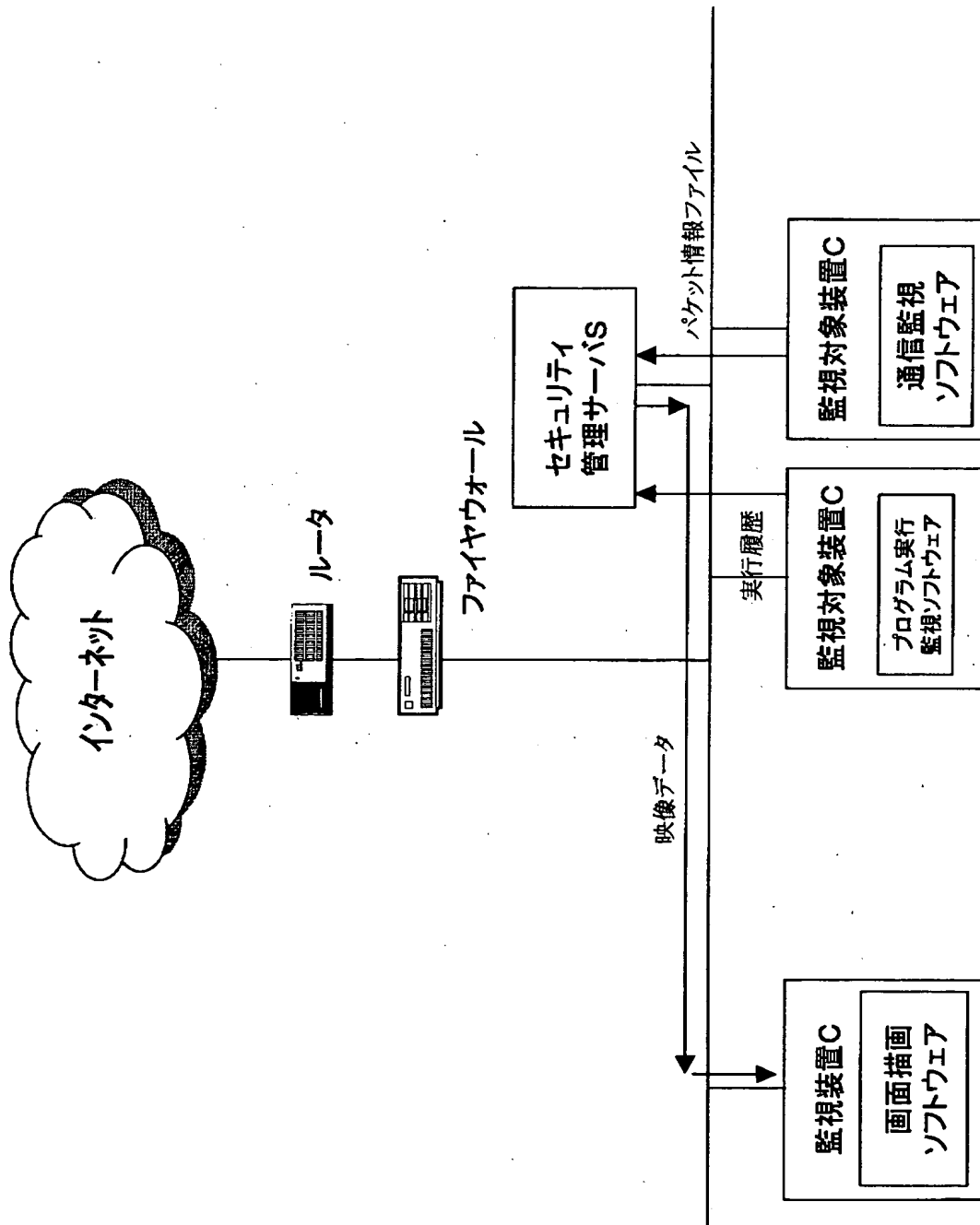
【図 8】



【図9】

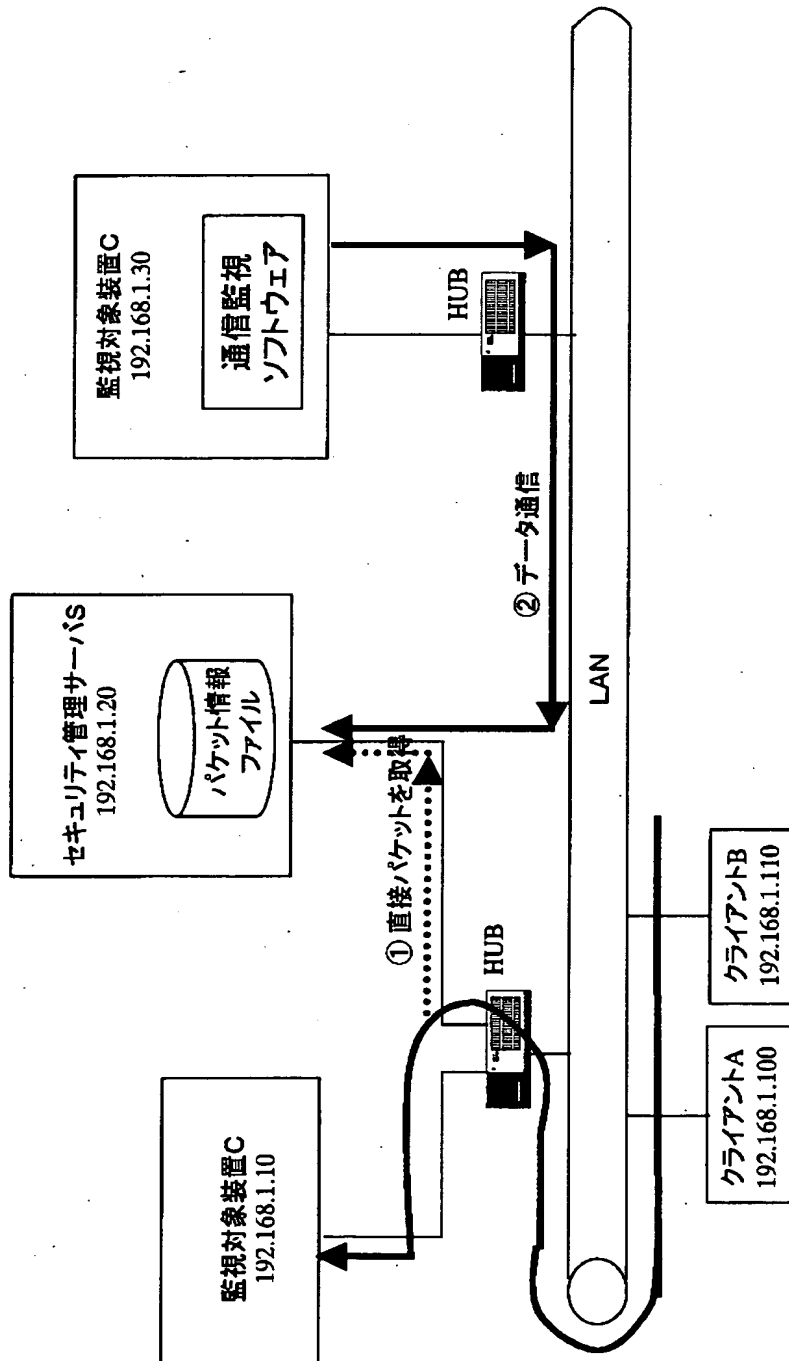


【図10】





【図 11】



- ① セキュリティ管理サーバと同一HUBに接続されている監視対象装置Cの通信パケットは直接取得可能
- ② セキュリティ管理サーバと異なるHUBに接続されている監視対象装置Cの通信パケットは、監視対象装置C側で蓄積記憶しておき、これをLAN経由のデータ通信により適宜セキュリティ管理サーバSに集信する。

【図 1 2】

## パケット情報ファイルのデータフォーマット

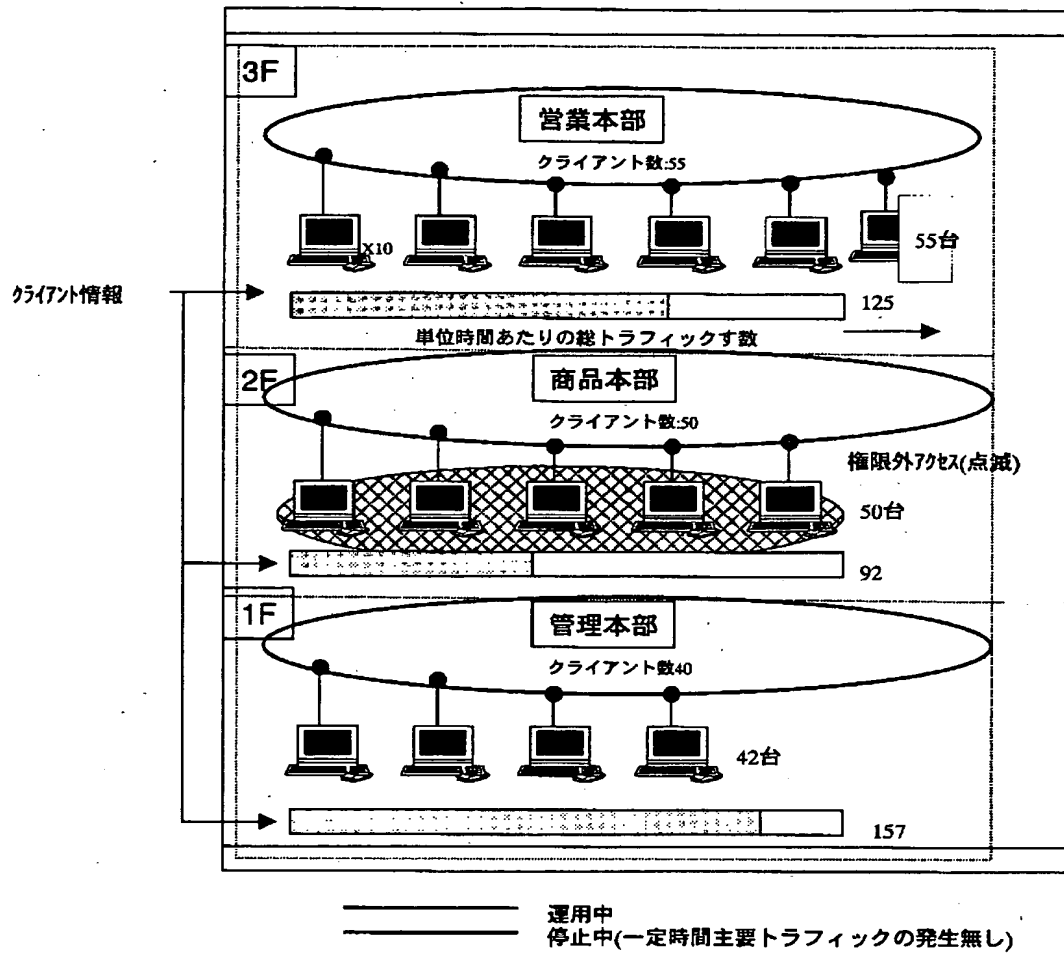
フィールド名	説明
time	収集時間(サーバー時間)
btFlags	フラグ 0:IN 1:OUT (サーバーから見て) 2:SMB(共有ファイルアクセス等)
wLength	パケットのオリジナル長
mwMac	クライアント MAC アドレス
dwIPAddr	クライアント IP アドレス
wPort	サーバーポート番号
btDataLength	パケットの可変データ部分の長さ (0から255)
btData[256]	256パケットの可変データ(可変長)

【図 1 3】

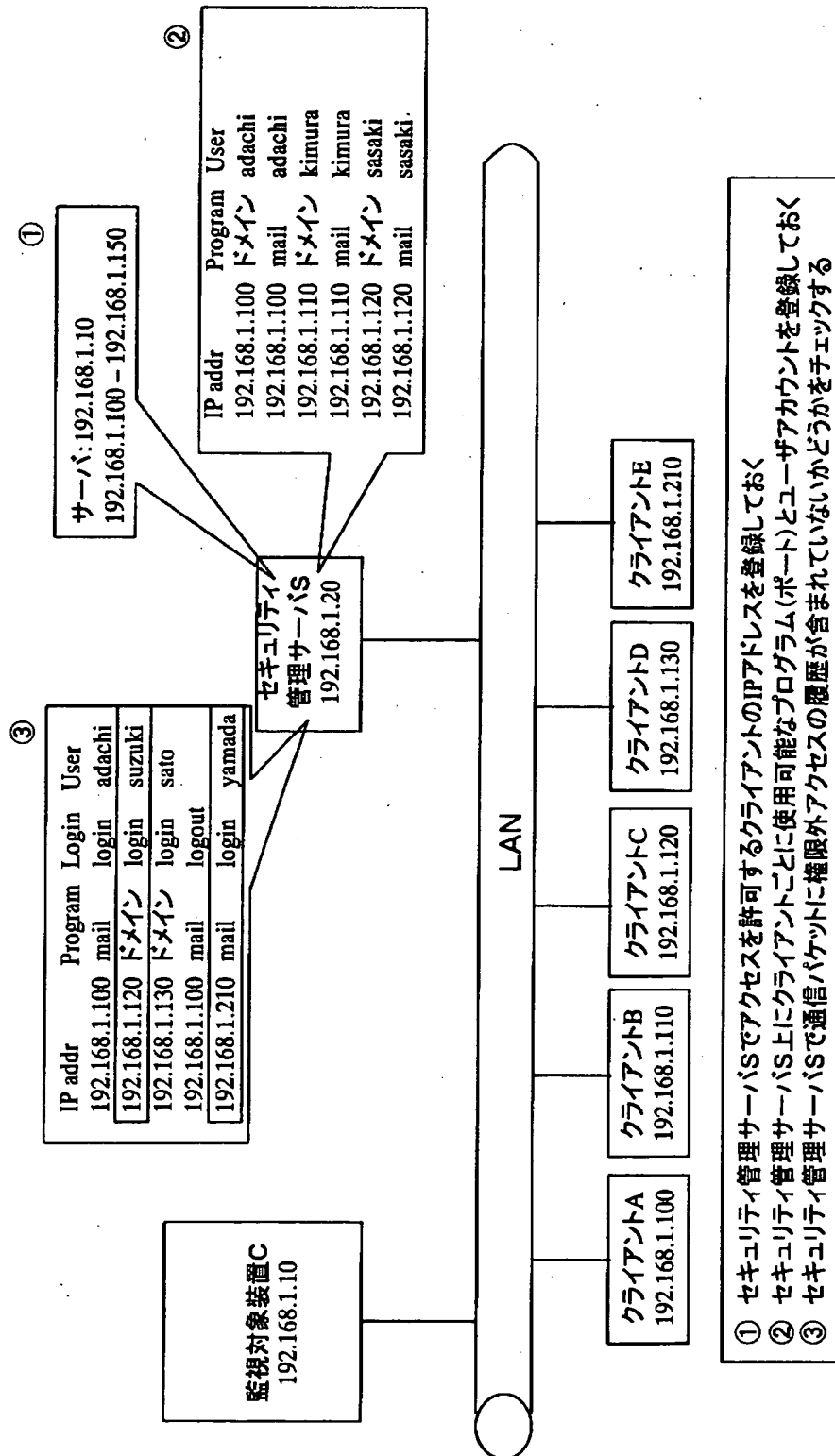
## 視覚化基礎データ

フィールド名	説明
time	収集時間(セキュリティ管理サーバでの時間)
wServerID	監視対象サーバー識別子
wType	パケットのタイプ (01:Login...65:Mail...)
mwMac	クライアント MAC アドレス
dwIPAddr	クライアント IP アドレス
wOriginalLength	パケットのオリジナル長
btData[256]	256パケットのタイプ別文字データ (Login:UserID/Mail:from.to...)

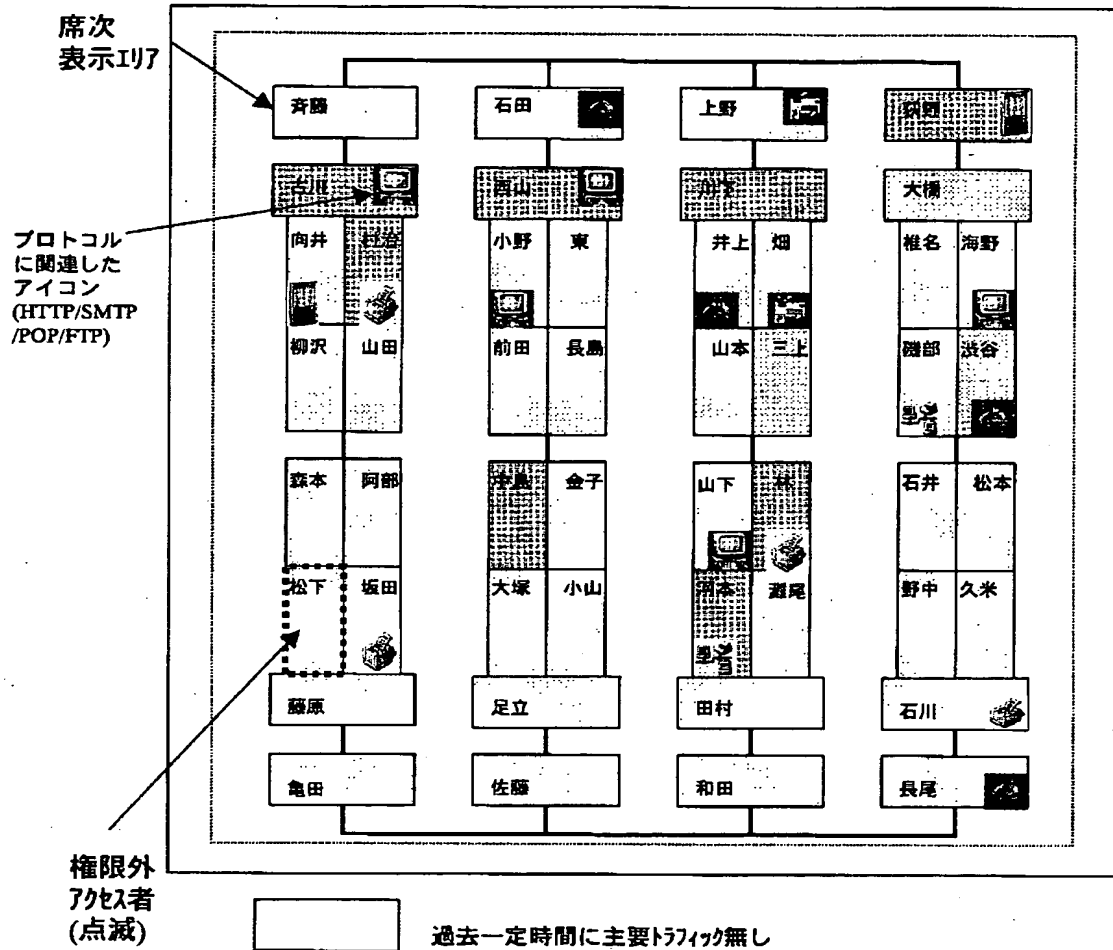
【図14】



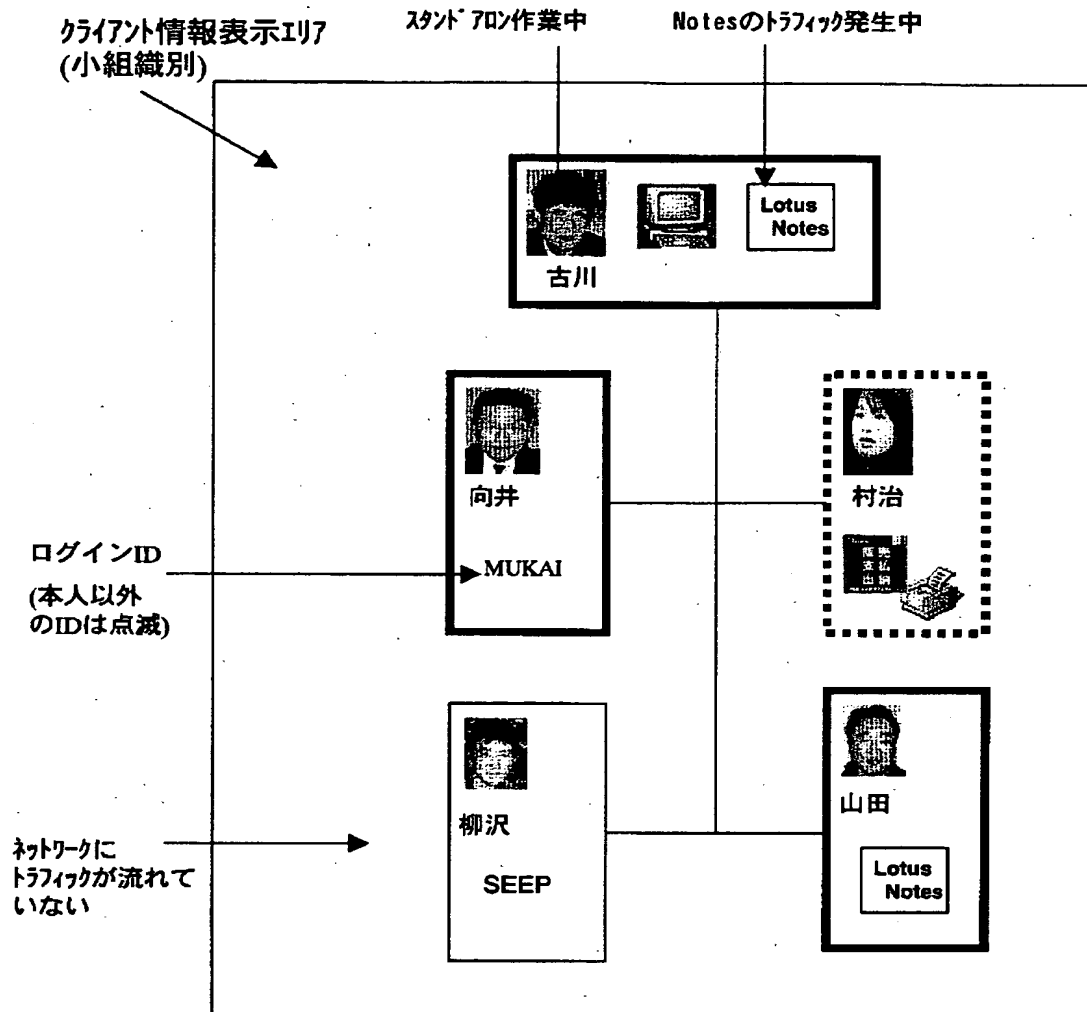
【図 15】



【図16】



【図17】



# クライアント情報画面

**利用者: Senri Yamada**

ステイタス:



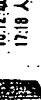
● 五一劳动节

氏名:	山田 千星	所属1:	営業本部	所属2:	金融商品企画部	役職:	課長
IPアドレス:	202.10.181.89	E-mailアドレス:	yanada@seer				

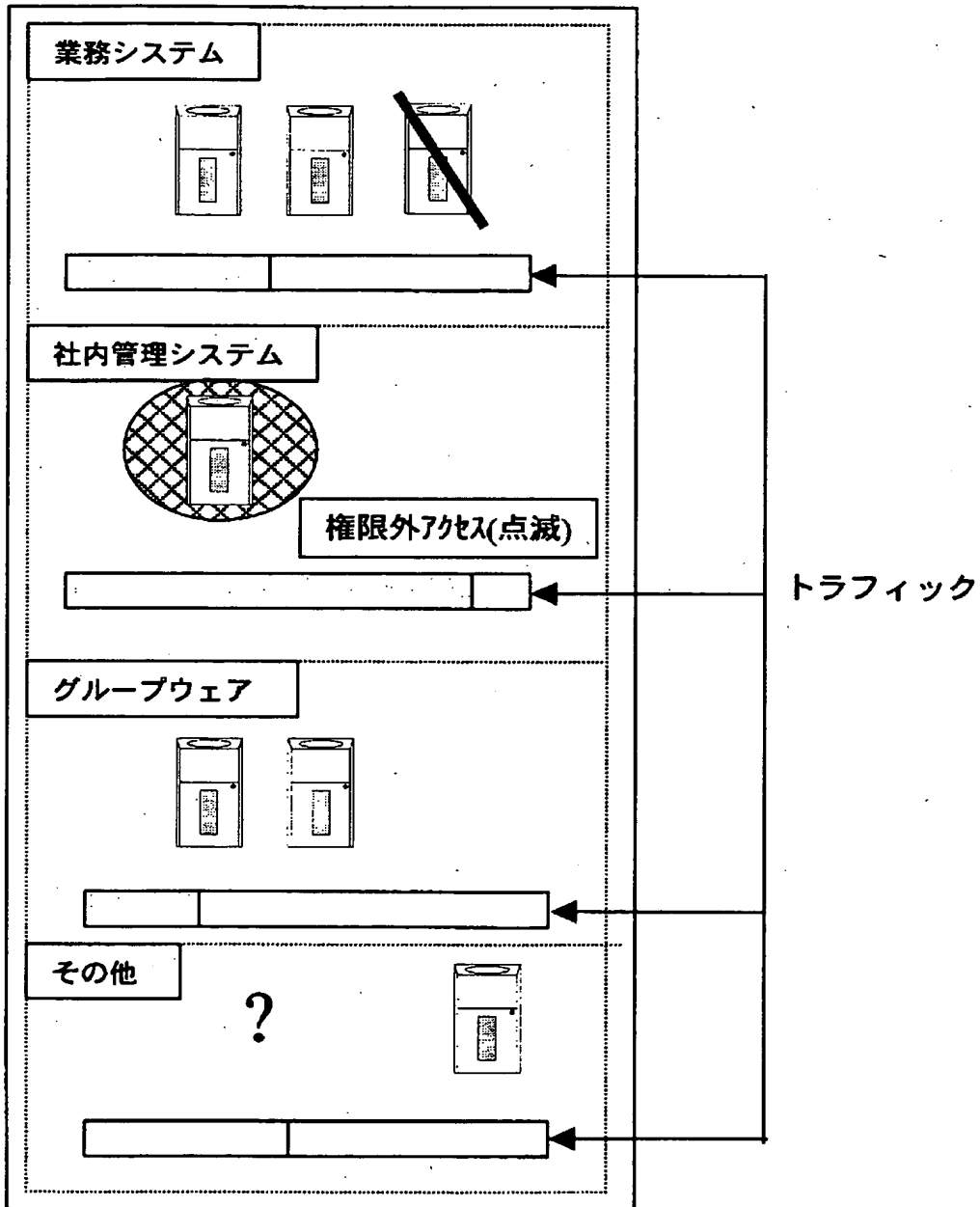
## ●システム情報：

情報システム:	Notes	顧客管理システム	市場予測システム	ワークフロー:	Office 2000
利用システム:	顧客DB	取引先DB	人事DB		
DB利用権限:	3:閲覧	2:更新	4:部分閲覧		

● 利用情報 ☐過去1時間 ☒本日履歴 ☐月 ☐日 履歴

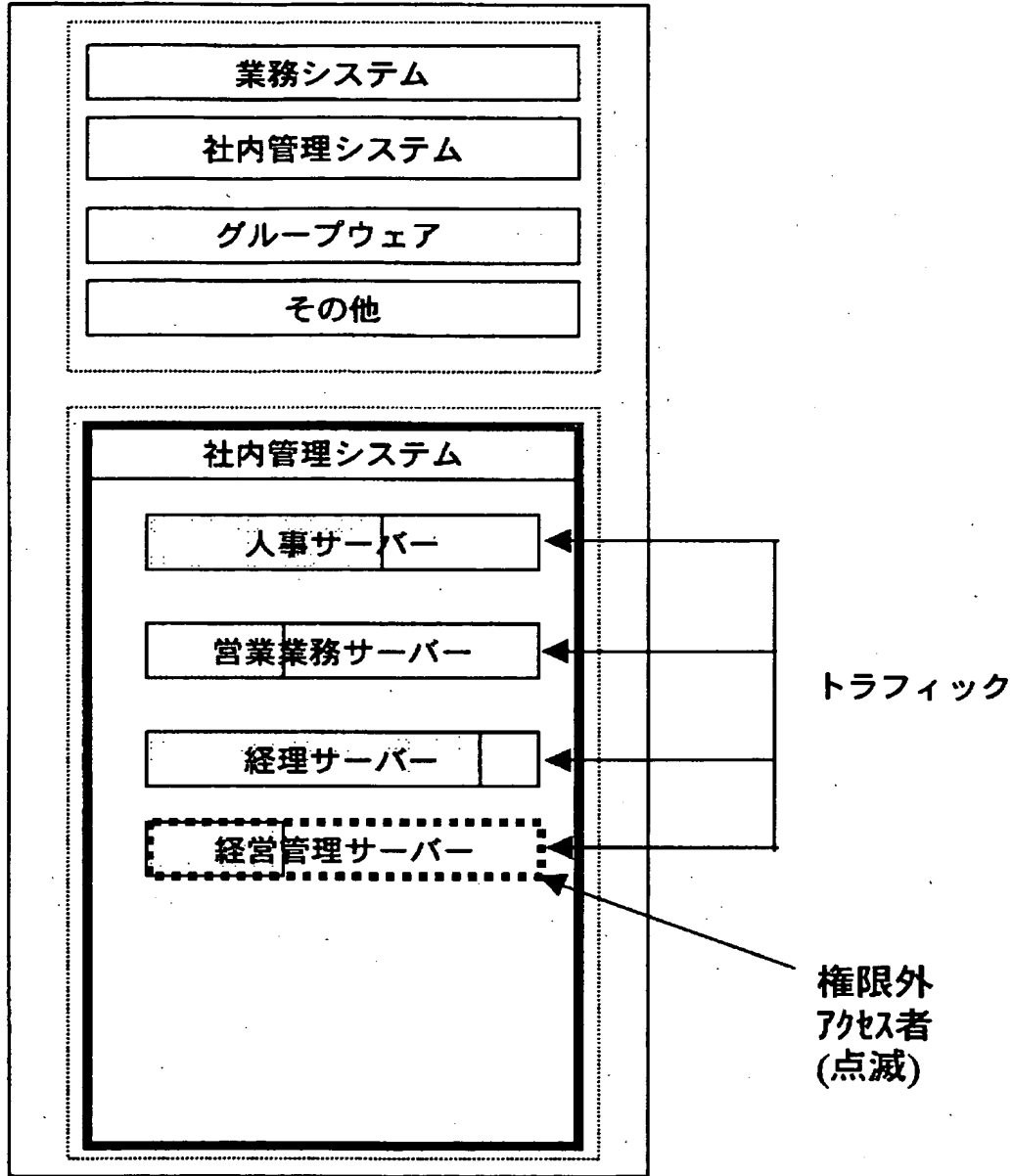
 <p>ネットワーク がイン</p>	<p>8:20 Office</p>	<p>8:20 Office 8:30 I&amp;E 8:31 qto 8:32 Gitech 9:00 e-track</p>	<p>8:25 news.doc 8:35 web</p>	<p>9:15 From Ishihara@ 9:15 To: maki@ 9:25 To: satou@</p>	<p>9:45 From Ishihara@ 9:45 To: maki@ 9:55 To: satou@</p>
<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>
<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>
<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>
<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>
<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>	<p>8:25 news.doc 8:35 web</p>

【図 19】

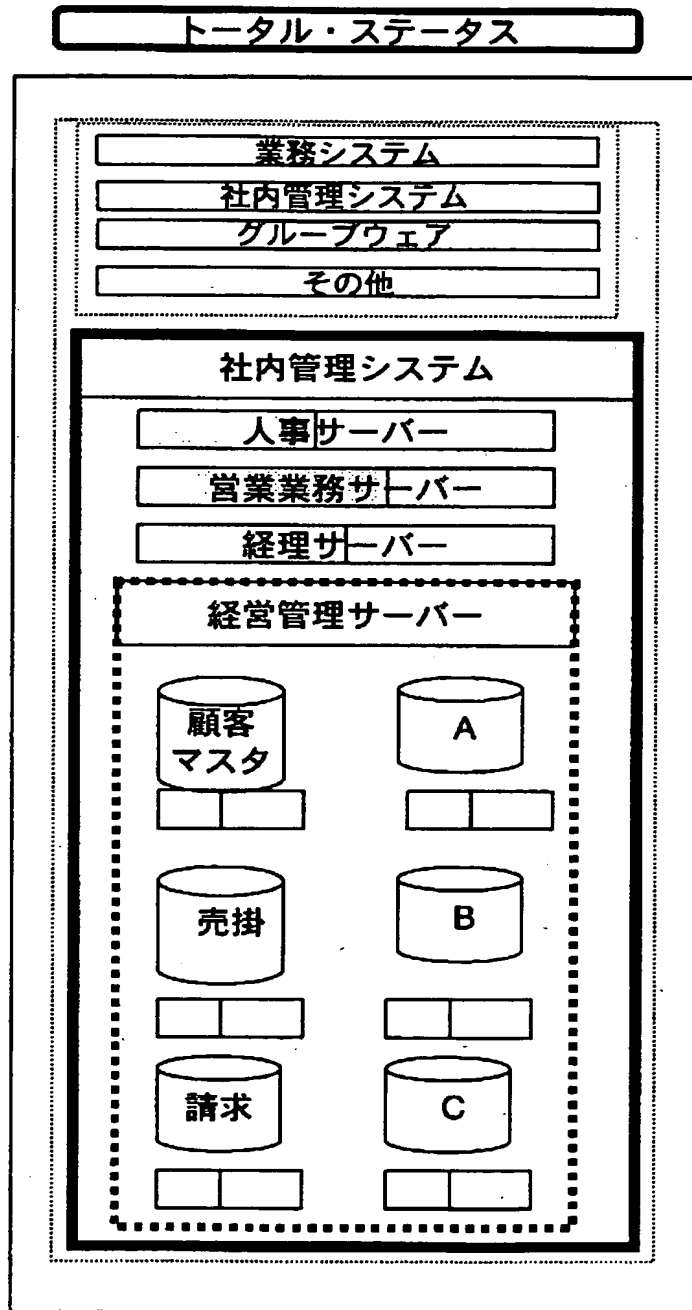




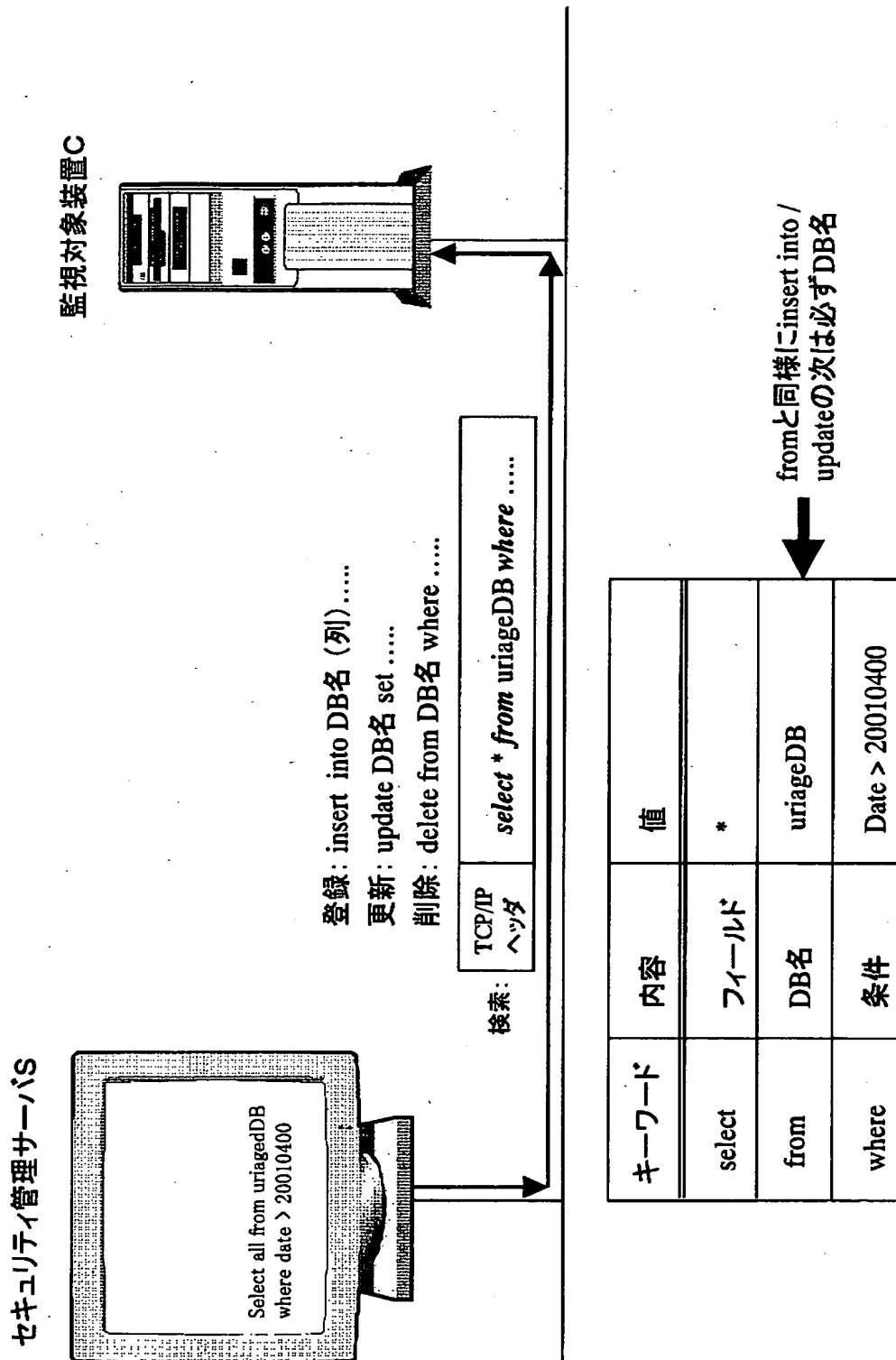
【図 20】



【図 21】



【図 22】



【書類名】 要約書

【要約】

【課題】 LANにおける各種のセキュリティサービスを提供するセキュリティ管理サーバおよびこれと連携して動作するホストサーバを提供する。

【解決手段】 インターネットなどの外部のネットワークに接続するLAN内に、LAN内で稼働する各種監視対象装置C内で管理されている各種のログ情報を収集する機能、収集したログ情報からLANのセキュリティ管理に有用な情報を抽出してこれを人が利用しやすい形態に視覚化した映像を生成する機能、前記映像を他の監視装置Cに送信する機能を備えたセキュリティ管理サーバSを設置する。また、セキュリティ管理サーバSは、外部のネットワークで稼働するホストサーバHと連携して各種のセキュリティサービスを提供する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [501051516]

1. 変更年月日 2001年 2月 6日

[変更理由] 新規登録

住 所 東京都港区南青山一丁目15番22号

氏 名 シーア・インサイト・セキュリティ株式会社